2025 Face Liveness Market Report and Buyer's Guide

by Biometric Update and Goode Intelligence

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

02 Executive summary
03 Introduction to face liveness
05 Standards and testing
10 Advancing the state-of-the-art
13 Pioneering providers
22 Market analysis and forecast
33 Face liveness buyer's guide
34 What to look for in a vendor
36 Vendor Profiles & Case Studies
iProov
Jumio
Mobai
Oz Forensics
Paravision
RealSense
Regula
Youverse
48 Vendor directory

2025 Face Liveness Market Report

Biometric face liveness detection is at the forefront of identity verification and authentication technology in 2025. Biometric Update and Goode Intelligence have partnered to create reports that demystify the market around the technologies that are of greatest importance to digital identity, detailing where gaps exist in how well market participants understand them.

Biometrics are generally used to prove a claim about an identity, but a match of an individual's biometrics is only as reliable as the data that is used to perform it. If the biometric data presented is not that of the individual it is presented as, then the transaction is an attempt to commit fraud known as a presentation attack.

'Liveness detection' is a term used in the field of biometrics to describe presentation attack detection and related assurances that the biometrics being matched are those of the correct individual. While the terms are often used interchangeably, liveness detection is somewhat broader, including the possibility of determining that an individual is sleeping or otherwise prevented from consenting to the presentation of their biometric data.

While liveness detection is broadly used in biometrics, its primary application in the market is the protection of user onboarding and authentication transactions against spoof attempts through face biometrics.

This Biometric Update / Goode Intelligence report explains the key concepts in facial liveness detection, presenting the commercially available technologies that organizations can implement to perform it, and guide those organizations in selecting a liveness detection provider.

The study also investigates the market for face liveness detection products and services, including adoption examples, sector and application analysis, and three-year forecasts for transactions and revenue.

About Us

This study has been created by a partnership bringing together Biometric Update and Goode Intelligence to produce analytical market reports stakeholders can use to make informed strategy, product and technology procurement choices.

Reports produced by the partnership are based on analysis of recent transactions and trends in the biometrics market, reviews of the regulatory, standards-development and competitive landscapes, and feedback from key insiders in each given area of focus.

Biometric Update is the world's leading source for daily news, opinion and insight into biometrics and digital identity.

Goode Intelligence is the world's leading independent biometrics market analyst and consulting firm, providing quality advice to global decision makers in business and technology.

Executive Summary

Liveness detection can protect face biometrics systems against spoof attacks, but not all liveness detection technologies do so equally well. There are different options available to organizations on the market in terms of approach to liveness detection, how they are integrated, and other key considerations. Understanding how those factors apply to your organization is critical to selecting the right provider for your specific use case and requirements.

Important factors to consider include:

Leading liveness detection providers are emerging from a crowded market

Accredited, independent testing can help guide procurement

Fraud attacks evolve over time, so liveness detection technologies and associated evaluations must do so too

Liveness detection is widely deployed to protect biometric systems against spoof attacks and to prove proof of personhood, and many of the commercially available products on the market are generally effective.

An ecosystem of international standards, accredited independent testing laboratories and ongoing research has grown up around liveness detection, contributing to the trustworthiness and overall quality of the technology.

The leading liveness detection algorithms can defend against most – but not all – fraud attacks, dramatically improving the security of biometric systems used for remote user onboarding and authentication.

This study provides a guide for buyers on what to look for in a face liveness detection supplier and identifies baseline criteria for measuring whether a face liveness detection solution is suitable.

The face liveness detection market is currently strong with demand especially high across sectors that are heavily regulated. The market is forecast to get stronger over the coming three years with revenue forecasts exceeding $252 million (USD) annually by 2027 – a CAGR of 36 percent over the three-year period.

Introduction to Face Liveness

What is face liveness detection

Whereas face biometrics is concerned with verifying or authenticating a person's identity, liveness concerns itself with **confirming that a person is real – not a fake**. This is also referred to as **proof of personhood**.

Face liveness detection is a security feature used in biometric systems to ensure that the biometric sample (like a fingerprint or facial image) is from a live person and not a fake representation. This technology helps prevent spoofing attacks where someone, or something, might try to deceive the system to commit fraud using photos, videos, masks, or other fake artifacts. Increasingly, these attacks are driven by artificial intelligence (AI).

Fraudsters have been known to use a variety of methods to try to trick biometric systems, including:

- High resolution 2D imagery
- Deepfakes
- 3D masks
- Wax heads
- Video or audio recordings
- Photocopies or other non-original documents

How does liveness detection work

Specific liveness detection methods differ between suppliers, but generally the technology looks for signs of fakery, such as: artificial skin tone, moiré noise, intensive glare, and unusual shadows. It uses AI to detect if a user is a real person, a replica or fictional identity.

Liveness detection works by:

Training: Systems are trained on large datasets of real-face images

Analyzing: Systems analyze the biometric sample for signs of artificiality

Comparing: Systems compare the sample to what is expected

Detecting: Systems detect anomalies, such as differences in tone, or spectral characteristics

What is Personhood?

In the context of liveness detection, **personhood** refers to verifying that a real, live human being is present during an authentication process, rather than a fake representation like a photo, video, mask, or synthetic digital creation. This is crucial for ensuring the security and integrity of biometric authentication systems.

Liveness detection can be divided between two types of approach:

- **Active Liveness Detection:** This requires the user to perform specific actions, such as blinking, smiling, or moving their head, to prove they are real.
- **Passive Liveness Detection:** This method analyzes the biometric data without requiring any action from the user. It uses algorithms to detect subtle signs of life, such as skin texture or blood flow, and signs of spoof attacks, such as pixelation or inconsistent shadows.

Where is liveness detection being used?

Liveness detection is used in many scenarios including:

Digital Onboarding: Taking a selfie as part of the digital onboarding process and to support AML and KYC processes / regulation

Biometric Authentication: Comparing the presented biometrics to a stored version (template)

Document Authentication: Liveness detection can be used to verify documents during onboarding

Account Management: Ensuring that it is a real person requesting password resets or new device setup

Why is it so important?

Liveness checks help companies protect themselves from fraud, identity theft, and other illegal activities. They are also a way for businesses to comply with KYC regulations, which can have serious consequences for non-compliance.

Face liveness detection is a critical component of identity assurance in an age of ever-increasing AI-driven fraud. Visa said that the number of charges on its credit-card network blocked for potential fraud on Black Friday and Cyber Monday 2024 surged 200 percent globally from 2023, with the card network attributing this increase to scammers using AI. Michael Jabbara, global head of fraud services at Visa was quoted in the Wall Street Journal "It is absolutely a golden age for fraud and fraudsters."

Standards and Testing - How is Face Liveness measured

Biometric face liveness detection is significantly newer than facial recognition, and the businesses that have made major contributions to the field are all still commercially active. The challenges facing liveness detection providers have evolved over the past two decades, with generative artificial intelligence and adversarial networks making spoof attacks both more sophisticated and easier to carry out.

Deepfakes, for instance, are not mentioned in ISO/IEC 30107-3, though liveness detection systems have proven adept at identifying AI-generated images that easily fool human analysts.

Liveness detection standards

The main standards for testing liveness detection are the ISO/IEC 30107-3:2023 standard and certain FIDO certifications.

The standards establish definitions and terminology, provide information on specific types of attacks, describe detection mechanisms, set appropriate testing conditions, and present error rates.

ISO/IEC 30107-3:2023

ISO/IEC 30107-3:2023 sets criteria for evaluating biometric presentation attack detection (PAD). The standard discusses different attack types, and tests based on it are typically carried out according to three classifications of attacks, though the standard does not categorize attack types.

Level 1: Includes basic attacks that use easily accessible equipment, such as printed photos, video, or dusted fingerprints.

Level 2: Includes more sophisticated attacks that require more preparation time and tools, such as 2D or 3D paper masks, fingerprint casting, or face demonstrations.

Level 3: Includes the most complex attacks that require the most preparation time and professional equipment, such as elaborate silicone masks.

An emerging standard for biometric injection attack detection, ISO/IEC NP 25456, is in development and something to consider when evaluating face biometric and liveness detection solutions. It is expected that the standard will define injection attack instruments and include a test plan for evaluating injection attack detection

systems. It is anticipated that the standard should reach the stable draft stage by January 2026.

FIDO Biometric Certification

FIDO Biometric Certification is based on ISO standards. There are two biometric evaluation certification programs:

1. **Face Verification Program** of remote biometric identity verification technology (verifying a user against a trusted identity document) to test and certify the performance for accuracy, liveness, and bias.
2. **Biometric Component Certification Program** of biometric verification technology (authentication of users) to test and certify the performance of biometric verification technology and considers accuracy, liveness, and bias.

Who certifies and confirms compliance for liveness products?

There are independent biometric testing authorities that certify liveness products against the two major standards. Biometric testing authorities must be accredited.

ISO/IEC 30107-3 is accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and FIDO Biometric Certification is accredited by the FIDO Alliance.

This study explores liveness certification and compliance testing authorities with exclusive interviews with leading test labs.

Independent, accredited liveness testing laboratories

Independent testing by accredited biometrics laboratories is crucial to understanding how effective liveness detection technology is at catching different kinds of spoof attacks. Each one tests for compliance to the ISO/IEC 30107 standard for presentation attack detection. There are a number of qualified labs across the world, several of which offered their insights through exclusive interviews for this report into the importance of testing, common misconceptions and how to engage in productive evaluations.

- **Ingenium Biometrics (UK)**
- **iBeta Quality Assurance (USA)**
- **Fime (France)**
- **BixeLab (Australia)**

Liveness testing is 'table stakes'

The labs consulted by Biometric Update and Goode Intelligence were unanimous that independent testing to the ISO standard for liveness detection should be considered 'table stakes' for providers, at this point in the technology's maturity.

Such testing provides "a baseline," according to iBeta Quality Assurance. It should not be the only thing considered but gives prospective customers some assurance about vendor claims.

Fime notes that some providers still perform only internal testing, due to "a lack of market mandates." That internal testing may leave some vulnerabilities undiscovered and make comparisons between providers difficult.

Ingenium Biometrics reminds customers selecting liveness detection technology to not blindly accept sales pitches.

BixeLab and Ingenium each note that for supervised and in-person biometrics enrollment or identity verification, liveness detection often does not carry the same importance as in unsupervised and remote processes.

- **Independent testing provides a 'baseline'**
- **Necessary for remote, unsupervised applications**

Liveness testing providers

The following table provides a curated list of independent biometric test labs.

ACCS	**iBeta**
BixeLab	**Ingenium**
CLR Labs	**ServeLegal**
FIDO Alliance	**Swiss Center for Biometrics Research and Testing**
Fime	**Tayllorcox**
Fraunhofer	

Top misconceptions

The top misconception about PAD testing among liveness providers is that simple attack types can be easily detected and therefore can be disregarded, iBeta says. In fact, it is often simple attacks that defeat liveness detection systems.

Fime notes that test results eventually become outdated, as attacks and the technologies used to detect them evolve. The French laboratory also identifies effective integration between the system's different components as a key to working properly in the field.

"Further analysis and testing can be required during the organizations' purchase process to adapt to the operational use case."

A liveness detection test does not necessarily provide much insight into performance in different operations and use cases, Ingenium notes. A system may behave quite differently using a reference image from the NFC chip of an identity document compared to a photo of the ID.

Detection of different presentation attack instruments (PAIs) can also vary between demographics, Fime cautions.

Ongoing and scenario-specific testing are necessary to ensure liveness detection is effective for its current, real-world application, BixeLab states.

- **Testing systems for vulnerability to sophisticated attacks is not enough**
- **Standard compliance is not a complete picture of effectiveness**

What to look for after standards compliance

Picking up on Fime's point about the field changing over time, iBeta emphasizes the importance of vendors proactively updating their algorithms, carrying out research and constantly monitoring their systems to catch any errors.

Ingenium likewise suggests that compliance testing for PAD standards five years ago may not be relevant today, which is why FIDO certification comes with a three-year limit.

Liveness vendors and customers alike also need to understand the limits of a given test. Injection attacks, for instance, are outside of the scope of ISO 30107, though a new standard for injection attack detection, ISO/IEC NP 25456, is in development.

'Bake-off' style tests can also help organizations implementing liveness detection to make a final decision about which provider to use.

Accurate face biometrics matching is another basic indicator to consider. Fime points out that FIDO includes bias evaluations, with performance differentials as an optional metric, and the lab also lists protection against deepfakes and injection attacks as important considerations.

BixeLab lists real-world performance metrics, ease of integration and scalability, and post-deployment support as important considerations, and echoes Fime's earlier point about integration, suggesting it should also be independently tested. Adaptability to new threats is another key characteristic to look for, which also informs BixeLab's advice on questioning liveness providers.

- **Proactive updates are necessary to keep up with evolving threats**
- **Don't neglect matching accuracy, usability and other key requirements**

Risk of complacency

The technology is mature, but also "re-learning" with AI as its backbone, iBeta argues. The shift comes with the potential for significant further improvement. BixeLab, similarly, assesses the technology as "relatively mature but still evolving."

Ingenium assesses the technology as mature in the sense that there are many generally effective options available on the market, but warns against the risk of complacency, referring to the phenomenon of unsophisticated attacks defeating sophisticated systems that iBeta mentions among misconceptions.

Face biometric liveness detection is mature compared to other modalities, Fime says, but must continue evolving to stay ahead of deepfakes and injection attacks.

- **Facial liveness detection is a relatively mature technology**
- **Changes in threat landscape make complacency dangerous**

Pioneering Face Liveness

What is a Liveness Pioneer?

The Pioneers of face liveness detection are developers that have advanced the state of the art in liveness detection through research and successful participation in novel or ground-breaking evaluations. It is thanks to those research initiatives and independent assessments that relying parties can be assured that effective facial liveness detection software, properly implemented, will protect against most spoof attacks.

By carrying out and collaborating on prominent liveness research, Pioneering vendors have demonstrated a proactive approach to liveness detection, which is necessary to ensure that effectiveness against attacks observed in the past will carry over to the improved spoofs and new presentation attack types that are constantly introduced.

Businesses selecting a liveness detection provider should consider the developers that have advanced the state of the art -- the 'Pioneers' of biometric liveness detection -- because the challenge they address is a dynamic one. As such, those engaged in ongoing research and development are more likely to maintain or improve their effectiveness over time.

Pioneering facial liveness detection providers were identified through analysis of more than 50 developers, based on their contributions to innovation in the space, proprietary technologies, usability and market success as reflected in Biometric Update's daily coverage of the biometrics industry.

Advancing the state-of-the-art

BioID was granted a patent for a challenge-response liveness detection system in 2004, and remains one of the industry's leading developers of defenses against spoof attacks. Today, BioID offers a combination of active and passive liveness detection.

FaceTec developed a method of 3D liveness detection using normal 2D cameras found on personal electronic devices like smartphones, ZoOm, which launched in 2017. The company now supplies 3D liveness detection to over 100 partners, and through them to numerous businesses, including household brand names.

iProov has one of the market's most recognizable methods of liveness detection, in the form of its patented 'Flashmark' technology, which flashes a sequence of colored lights at the subject and measures their reflection. The company's Dynamic Liveness is also the first to complete FIDO Face Verification certification.

BASF subsidiary **trinamiX** has also developed 3D sensing technology for liveness detection. TrinamiX uses

specialized hardware to detect human skin as a way to prevent spoof attacks on biometric systems.

These early pioneers in facial liveness detection helped to establish the technology as a valuable technology for detecting and preventing fraud. Over the past several years, the state of the art in liveness detection has continued to evolve to address targeted attacks against face biometrics systems and common challenges in facial recognition, and to pit systems against each other in independent performance evaluations.

Independent testing and research

ID R&D, a **Mitek** company, commissioned the industry's first-ever independent assessment of demographic bias in liveness detection from BixeLab in 2022. The evaluation showed fair performance across demographic groups. Similarly, **Daon** provides liveness detection to Identity Check app for access to government services, through its IdentityX platform. BixeLab tested the system for accuracy with New Zealand's different demographics, including Māori and Pasifika users. Despite a lack of training data for these demographic groups, Daon's liveness detection was found to be accurate for all groups.

Mobai is a spinoff from the Norwegian University of Science and Technology (NTNU) which developed a biometric authentication solution that draws on the expertise of researchers prominent within the field to perform liveness detection on face, iris and ocular biometric modalities. Among the combined technology's capabilities, it can detect morphed photographs from a single image.

Facial liveness detection is also intersecting with other trends in biometrics, being implemented in novel architectures and integrated into emerging use cases. **Youverse** has designed its facial liveness detection with a decentralized architecture for what the company says is a privacy-preserving, zero-knowledge approach to biometric authentication. In addition to passing independent PAD evaluations, Youverse also claims to be the only vendor offering decentralized authentication backed by strong performance in NIST face biometrics evaluations. **Yoti** has integrated facial liveness detection with its age estimation software to provide online age checks with assurance against spoof attacks, and carried out extensive research into demographic bias.

The USA's National Institute of Standards and Technology held its first independent evaluation of passive PAD systems in 2023, assessing algorithmic performance against different types of tasks and attack types.

NIST evaluated 82 algorithms from 45 developers for their convenience, as measured by attack presentation classification error rate (APCER), and security, as measured by bona fide classification error rate (BPCER), each with the other set at 0.01.

With certain presentation attack types, **Aware** had the lowest BPCER when detecting both impersonation and evasion in still images, making it the most secure among those tested for the use case. **CyberLink** had the lowest ACPER for the same attack type, and also topped several other categories. **Onfido** had the lowest APCER for type 3 PAs for evasion detection with still images and **ROC** had the lowest APCER and BPCER for evasion detection with type 6 attacks.

iProov and ID R&D also took first in individual categories in the evaluation.

Another participant in the NIST evaluation, **Neurotechnology**, has contributed research into the benefit of building image quality metrics into liveness detection systems.

The USA General Services Administration (GSA) built biometric liveness detection into its SSO service for access to government programs in order to meet the compliance requirements for Identity Assurance Level 2 (IAL2), as defined by NIST, and stem a tide of fraud against public services. GSA evaluated five liveness detection vendors, with mixed results. Among the developers trialled, **LexisNexis Risk Solutions**, **Socure** and **Incode** have been certified for IAL2 by the Kantara Initiative, and **Jumio** is a Registered Applicant, with final approval pending. The GSA's study results are expected to be published in 2025.

America's Department of Homeland Security's Science and Technology Directorate (S&T) held a Remote Identity Validation Technology Demonstration (RIVTD) track assessing liveness detection software in 2024. The assessment found that the performance of liveness detection software from different vendors can vary significantly and presented anonymized results. One vendor that has revealed its results is **Idemia Public Security**, which was the only one to meet the benchmark set by DHS S&T for performance, speed and customer satisfaction on both iOS and Android devices.

These and other developers have brought liveness detection to the point it is at today, as a necessary tool to defend organizations and users against online identity fraud.

Pioneers of face liveness detection

The Pioneers of face liveness detection are the biometrics providers that have demonstrated an ability to prevent biometric spoof attacks and advance the maturity of the field. They have been selected from a candidate list of more than 50 liveness vendors based on an analysis of technical criteria, business stability and market position.

Each Liveness Pioneer has passed an independent evaluation by an accredited biometrics laboratory, established a reputation as a credible biometric technology provider, and shows a sustainable business model. They tend to have intellectual property protection for their proprietary technology, and either major market share, a unique niche within the market, or both.

The suitability of a face liveness detection provider to a given application depends on both the overall effectiveness of the technology and its fit with the specific requirements of the use case.

Aware

Aware, Inc. is a company founded in 1986, headquartered in Burlington, Massachusetts, USA and publicly traded on the Nasdaq. The company specializes in biometrics software products and solutions, providing authentication services for government agencies and commercial entities worldwide.

Aware integrates liveness detection into its biometric authentication solutions which cater to various industries including financial services, enterprise, healthcare, gambling, law enforcement, and border management, enabling secure identity verification and management.

The company has stable financial footing, with more than half of its revenues recurring, and a significant market share, particularly in the United States. A new CEO appointed early in 2025 brings a track record of success working with prominent American public and private-sector organizations.

Aware is also expanding internationally, and targets developers with tools for popular platforms like WordPress and WooCommerce.

Both active and passive face liveness detection are offered by Aware, and it has passed a Level 2 PAD assessment from iBeta. The company holds numerous patents, several of which are directly related to liveness.

BioID

BioID GmbH is a private company founded in 1998, originating from a research project at the German research institute Fraunhofer IIS and headquartered in Nuremberg, Germany. BioID specializes in biometric authentication software, offering services such as facial recognition, certified liveness detection, and periocular recognition.

Its solutions cater to various industries, including financial services, enterprise, healthcare, and government organizations, providing secure and

convenient identity verification and authentication. BioID's liveness detection is also widely implemented by identity verification providers, contributing to a leading worldwide market share.

Customers of BioID can choose active or passive liveness detection. The company's technology is patent-protected and has passed a Level 2 (or 'B') PAD assessment by Germany's TÜV Informationstechnik GmbH (TÜViT). BioID offers its technology as a web service, and a Deepfake Detection API was added to its face liveness detection in 2023.

BioID is a regular contributor to industry workshops held by the European Association for Biometrics (EAB) on the topics of liveness detection and deepfakes, and has a leading market share in Europe and around the world, with additional offices in the USA.

CyberLink

CyberLink Corp. is a publicly traded company founded in 1996 and is headquartered in New Taipei City, Taiwan. CyberLink specializes in multimedia software and AI facial recognition technology, offering a range of solutions for digital content creation, multimedia playback, video conferencing, live casting, mobile applications, and AI facial recognition. CyberLink integrates liveness detection into its facial recognition platform FaceMe.

CyberLink's software supports both active and passive liveness detection. The company's algorithms use 2D analysis with standard cameras found in mobile devices and webcams or 3D analysis with specialized depth cameras, and can combine infrared (IR) and standard RGB cameras for enhanced anti-spoofing.

The company is well-capitalized and profitable, with significant market share, and holds multiple U.S. patents related to liveness detection. Target markets include the financial services, education, OEM and enterprise verticals.

CyberLink has passed Level 2 compliance testing by iBeta, and also showed strong performance in terms of convenience and security in NIST's PAD evaluation.

Daon

Daon is a private company founded in 2000 and headquartered in Fairfax, Virginia, USA, with additional operations in Dublin, Ireland, and regional offices in Serbia and Australia. Daon specializes in biometric authentication and identity assurance solutions, and has a large global market share.

Daon integrates liveness detection into its biometric authentication solutions which are utilized across various industries including financial services, healthcare, public sector, retail, telecommunications, and travel, to provide secure and convenient identity verification and authentication services.

The company utilizes passive liveness detection, protected by more than a dozen patents specific to face liveness detection, and has passed an iBeta Level 2 PAD assessment. Daon also develops liveness detection for other biometric modalities, and built deepfake detection algorithms into its IdentityX and TrustX platforms in 2023.

Daon also participated in a novel study of demographic bias in liveness detection with Australia's BixeLab to support an implementation by New Zealand's government.

FaceTec

FaceTec is a private company founded in 2013 and is headquartered in Las Vegas, Nevada, USA. FaceTec specializes in software that performs 3D "ZoOm" face authentication with regular 2D cameras, providing solutions for facial recognition and liveness detection.

Its technology is widely utilized across various industries, including financial services, border security, transportation, blockchain, e-voting, social networks, and online dating, enabling secure and reliable identity verification. The company is also involved in several mobile driver's license programs across the United States, and recently appointed a veteran federal law enforcement official to lead its public sector deployments. FaceTec is a global leader in liveness detection market share, performing 2.9 billion liveness checks annually.

The company's active 3D liveness detection has also been integrated with UR Codes, specialized biometric credentials that utilize the QR code protocol and can be presented digitally or printed on paper or plastic, further expanding its market potential.

FaceTec's patented liveness software is delivered from the cloud, with associated device-side SDKs, and is integrated into solutions and products by developers. It has passed a Level 2 PAD test by iBeta, and more recently another by BixeLab which included 3D-2D matching and analysis of demographic differentials. The company also runs a unique spoof bug bounty program to identify vulnerabilities before they cause real-world harm.

ID R&D

ID R&D was founded in 2016 and is headquartered in New York City, New York, USA. In 2021, ID R&D was acquired by publicly traded Mitek Systems, a provider of digital identity verification solutions.

The company specializes in biometric authentication technologies, offering solutions such as voice and behavioral biometrics, voice anti-spoofing, and passive facial liveness detection. These technologies are designed to enhance security while providing a frictionless user experience across various industries, including financial services, enterprise access control, healthcare, and telecommunications. ID R&D's focus on serving developers contributes to a strong market share, which is bolstered by Mitek's deep financial services ties.

The passive face liveness detection software provided by ID R&D's IDLive Face is patent-protected, and runs on the end-user's device.

ID R&D has completed a Level 2 PAD assessment from iBeta, and also a novel evaluation of the demographic fairness of its face liveness detection by BixeLab in 2022. The evaluation found consistent results for people of all genders, ages and races. ID R&D also scored the best result in one category of NIST's 2023 PAD report, and participated in the international LivDet-Face 2024 research project.

The company has also performed extensive research on detecting deepfakes and injection attacks with its PAD technology.

IDEMIA

IDEMIA is a French multinational technology company headquartered in Courbevoie, Île-de-France, France. It was formed in 2017 through the merger of Oberthur Technologies and Safran Identity & Security (formerly known as Morpho). IDEMIA Public Security is a subsidiary headquartered in Reston, Virginia, USA and serving North America's public sector market.

The French company is a large multinational enterprise, with three main divisions each serving different market segments. IDEMIA Smart identity is the division that provides identity verification, and therefore face liveness detection. IN Groupe is currently in exclusive negotiations to acquire IDEMIA Smart Identity.

IDEMIA specializes in identity-related security services, providing biometric identification products and software, including facial recognition systems, fingerprint and iris recognition, biometric terminals, e-gates, ID cards, ePassports, payment cards, and SIM cards. It has significant market share in face liveness detection and extensive geographic market reach.

IDEMIA's selfie liveness detection technology is available in active and passive models, and both models have successfully completed independent third-party evaluations for PAD Level 2 compliance from iBeta.

Both the France and USA-headquartered units of IDEMIA hold patents in face liveness detection.

In an evaluation of the operational performance of face liveness detection technologies in 2024, an algorithm from IDEMIA Public Security was the only one found by America's Department of Homeland Security's Science & Technology Directorate to meet the target benchmarks for speed, performance and customer satisfaction.

IDVerse

IDVerse, formerly known as OCR Labs Global, is a private company founded in 2014 and is headquartered in London, UK with additional offices in Sydney, Australia, Istanbul, Turkey and Silicon Valley, USA. LexisNexis is expected to complete the acquisition of IDVerse in early 2025.

The company specializes in identity verification solutions, offering services such as biometric verification, document fraud analysis, and face authentication. IDVerse serves the financial services, crypto, insurance, gambling, online marketplace and community, government services, mobility and telecommunications markets. The company has a strong market share, including through identity verification partners like OneID and Signicat, credit reporting services like Experian and identity and access management platforms like ForgeRock.

The proprietary, active face liveness detection provided by IDVerse is delivered through its Identity Verification and Face Access software products. Testing by BixeLab confirmed IDVerse's Level 2 PAD standard compliance and showed a 0 percent difference in demographic performance with its 'Zero Bias AI.'

Incode

Incode Technologies Inc. is a private company founded in 2015 and is headquartered in San Francisco, California, USA. The company raised $245 million dollars in series A and B funding rounds in 2021.

Incode specializes in identity verification and authentication solutions. Its platform is utilized by industries including financial services, government, retail, hospitality, and healthcare, enabling customers to validate their identity using face biometrics and government-issued IDs through web or mobile applications. The company has a significant market share in North America.

The proprietary ML model for passive liveness technology offered by Incode utilizes video, depth and motion sensors to accurately detect and prevent fraud by identifying physical spoofs like photo printouts and masks, as well as digital manipulations like AI-generated deepfakes.

Incode is a participant in the USA GSA's liveness detection evaluation, and its identity verification software has been certified to Identity Assurance Level 2 (IAL2) by the Kantara Initiative. The company's face liveness detection has also passed a Level 2 PAD assessment by iBeta. Evaluations by Michigan State University's Mobile Face Spoofing Database in 2023 and the Georgia Department of Driver's Services in 2024 each found 0 false positive and 0 false negative matches.

iProov

iProov is a private company founded in 2011 and is headquartered in London, UK. The company has raised a total of $78 million over a series of funding rounds, the last closed in 2022, and its high market share contributes to an apparently sound financial position.

iProov specializes in biometric facial verification technology, providing solutions for secure online identity verification and authentication. The company's services are utilized by governments, financial institutions, and enterprises worldwide, making iProov one of the global face liveness detection market leaders. iProov's face biometrics and liveness detection are embedded in Frontex' 'Travel to Europe' EES app, through the company's partnership with Inverid.

The passive face liveness detection offered by iProov utilizes its patented 'Flashmark' technology, in which the user's device produces a randomly-sequenced series of colored flashes of light. iProov also claims its layered approach to injection attack and deepfake detection, which includes its Flashmark technology, is effective against sophisticated attacks that can defeat other liveness detection systems.

iProov has successfully completed a Level 2 PAD assessment from iBeta, and its Dynamic Liveness is the first product to be certified to the FIDO Alliance's IDV Face Verification standard, with an independent test performed in 2024 by Ingenium.

Jumio

Jumio is a private company founded in 2010 and headquartered in Sunnyvale, California, USA, with offices and local subsidiaries around the world. The company has raised over $200 million dollars in a series of funding rounds which culminated in a $150 million round in 2021.

Jumio specializes in digital identity verification and authentication services, utilizing technologies such as artificial intelligence, biometrics, machine learning, and liveness detection. The company's technology is provided in comprehensive solutions delivered from a platform that cover the entire customer lifecycle.

Jumio's proprietary active liveness detection protects biometric systems from presentation and injection attacks.

Its solutions help organizations across various sectors, including financial services, digital currency, retail, travel, mobility, education, telecom and online gaming to onboard customers quickly, prevent fraud, and comply with regulatory requirements. Jumio has significant market share, notably in the financial services market.

Jumio has been confirmed for PAD standard compliance by iBeta. More recently, the company participated in the USA GSA's liveness detection trial and is a Registered Applicant for IAL2 certification by Kantara.

Mobai

Mobai is a private company spun out of the Norwegian University of Science and Technology (NTNU) in 2019, and is headquartered in Gjøvik, Norway. It has raised roughly $6 million in funding, through the completion of an oversubscribed seed round that closed in 2024, and has a growing share of the liveness detection market.

The company specializes in biometric face verification solutions, focusing on facial recognition, presentation attack detection, liveness detection, and morphing (deepfake) detection. Its SDK is designed to enable developers to build identity verification and authentication tools for service providers in regulated markets, such as financial services, healthcare and gambling, as well as government services.

Mobai continues to build on its strong background in biometrics research and development, which includes the invention of a novel system for detecting morphed facial images from a single image, with the support of prominent advisors Kiran Raja, Raghavendra Ramchandra and Christoph Bush.

The multi-modal passive liveness detection provided by Mobai uses a combination of face, iris and ocular biometrics, and has passed a PAD standard compliance test from Idiap's Swiss Center for Biometrics.

Onfido

Onfido, established in 2012, is headquartered in London, England, and has offices in India, the USA, France, Portugal and Singapore. It was acquired by Entrust Corporation in 2024.

The company specializes in digital identity verification and orchestration, with its face liveness detection built into its comprehensive Real Identity Platform. The Onfido identity verification suite includes 'Motion' active liveness detection and 'Selfie' passive liveness detection.

The company's target markets include financial services, compliance checks under the UK's DIATF, healthcare, e-commerce, gambling, sharing economy, telecom and transportation. It holds a leading share of the liveness detection market in North America and Europe.

Onfido holds multiple patents in and related to active liveness detection, and added acoustic face liveness detection to its software portfolio through the acquisition of Eyn in 2021.

Onfido has passed a Level 2 PAD compliance test from iBeta, and claimed the top spot in one of the security categories of NIST's 2023 PAD report.

Paravision

Paravision is a private company founded in 2013, headquartered in San Francisco, California, USA. It has raised $52 million through several funding rounds.

The company focuses on the ethical development of software related to face biometrics, including passive, single-frame face liveness and deepfake detection. The cloud software is integrated via Docker, though Paravision also provides an on-device video option.

Paravision's target markets include financial services, healthcare, government services, stadiums and events, payments and retail, gambling and the gig economy. The company's liveness detection is implemented mainly by integration partners like HID.

Face liveness detection from Paravision incorporates live feedback to the end user to help capture good quality images with minimal friction. The company launched an early USA-based commercial liveness detection product in 2018, under its previous brand name, Ever AI.

Paravision's updated liveness detection software, released to production in 2024, has passed a Level 2 PAD assessment from iBeta. The company's deepfake detection technology was developed over a multi-year collaboration with a Five-Eyes government, and also moved into production in 2024.

ROC

ROC (formerly Rank One Computing), established in 2015, is privately owned and headquartered in Denver, Colorado, with additional offices in Michigan and West Virginia.

It specializes in developing advanced biometric and computer vision solutions, including facial recognition, fingerprint recognition, iris recognition, and object detection. Its authentication software is delivered through an SDK.

The company serves the financial services, government and events markets, with a significant focus on supporting developers, and has a strong market share in North America.

ROC offers a patented single-frame passive liveness detection technology designed to prevent spoofing and fraud during identity verification processes without adding friction. ROC face liveness checks are completed in less than a second on any sensor, system, or device.

The software has passed a Level 2 PAD compliance assessment by iBeta, and ROC showed the best performance by both security and convenience criteria in one of the spoof categories in NIST's 2023 PAD report.

Socure

Socure, established in 2012, is a private firm headquartered in Incline Village, Nevada, USA, with a regional office in Chennai, India. The company has raised hundreds of millions of dollars in funding and says its transactions handled doubled from 2023 to 2024 to 2.7 billion identity requests.

Socure's software is delivered as integrated solutions. Its Predictive DocV product integrates passive liveness detection, and the company holds several patents related to user authentication and identity verification with liveness detection as a layer. Socure's liveness detection also includes deepfake detection and injection attack detection capabilities.

The company serves the financial services, government, gaming, healthcare, telecom, and e-commerce industries, and has significant market share in the USA, with prominent clients including Capital One, Citi, Robinhood and DraftKings.

Socure claims to have passed a Level 2 PAD compliance test, though without specifying the accredited testing laboratory, and is certified to NIST IAL2 by the Kantara Initiative.

trinamiX

trinamiX GmbH, established in 2015, is a wholly owned subsidiary of BASF SE, headquartered in Ludwigshafen, Germany.

trinamiX has developed a unique method of liveness detection that enhances biometric authentication security by detecting human skin with beam profile analysis using dedicated hardware and software. The company holds many patents for the beam profile analysis technology.

This passive liveness detection technique is integrated into its face authentication solutions for integration into consumer electronics by OEMs. The company primarily serves the automotive and mobile device markets.

As a hardware-based solution, trinamiX face liveness detection is subject to different testing regimes than the other providers covered in the report. The technology implemented behind an OLED display has been certified for compliance to the IIFAA Biometric Face Security Test Requirement and as a FIDO Level C Biometric Component.

Veridas

Veridas is a private company founded in 2017 by bank BBVA and industrial design company das-Nano and headquartered in Tajonar, Spain. The company has raised over $20 million in seed funding and a series A round completed in 2023.

It specializes in digital identity verification and biometric authentication solutions, offering proprietary technologies for facial and voice biometrics, identity document verification, and liveness and injection attack detection.

Customers can choose either active face liveness detection with randomized challenges to maximize security, or passive face liveness

detection for a seamless user experience.The liveness detection software is delivered through Veridas' ID Verification Platform or its Face Authentication solution, with sector-specific SDKs for easy integration, or built into its 'flow' facial access control platform.

The company targets the financial services, insurance, telecom, gambling, stadium and events, facilities, and public security industries.

Veridas' liveness detection has passed a Level 2 PAD compliance assessment from iBeta.

Yoti

Yoti is a privately held company founded in 2014, and headquartered in London, United Kingdom, with additional offices in the USA, Canada, Australia, India and New Zealand. It has raised over $50 million dollars through a series of funding rounds.

The company specializes in digital identity solutions, including identity verification, age estimation, and e-signatures. Its software is delivered through the Yoti ID app or integrated through a no-code portal, SDK and API.

Yoti's services are utilized across various sectors, such as financial services, social media, retail and e-commerce as well as UK compliance checks carried out under the DIATF to enhance security and streamline user authentication processes.

Yoti has developed a proprietary passive liveness detection solution called MyFace to ensure that the individual undergoing ID verification is physically present. Yoti also includes liveness detection in its facial age estimation solution.

The software has passed a Level 2 PAD assessment from iBeta.

Youverse

Youverse was founded in 2019 as YooniK before rebranding in 2023. It is a private company headquartered in Lisbon, Portugal.

The company specializes in developer-first facial biometric authentication solutions for various sectors from banking to hospitality. Youverse's passive liveness detection is delivered as part of its YouFace, YouAuth and YouID solutions, as cloud or self-hosted software, and integrated through native SDKs.

YouAuth is a decentralized authentication solution with deepfake detection utilizing a zero-knowledge architecture for enhanced privacy protection. Youverse is unusual among participants in NIST's face verification evaluation that offer liveness detection in its use of decentralized authentication.

The software's face liveness detection ensures users are physically present during the verification process for convenient sign-ins with resilience against fraud attacks.

Youverse has passed a Level 2 PAD assessment from iBeta.

Face Liveness Market Analysis & Forecasts

This section provides market analysis and forecasts for face liveness detection.

It investigates key drivers, adoption, key applications and sectors for face liveness detection.

The forecasts consider a three-year period, 2025-2027, covering:

1. Transactions
2. Revenue

Face liveness market analysis

This section investigates key drivers for adoption, important sectors, and applications for the adoption of face liveness detection, and adoption examples around the world.

Key drivers

The four key drivers for face liveness detection adoption are:

1. Fraud Prevention
2. Enhancing Security
3. Removing Friction
4. Improving Accuracy

Fraud prevention

Organizations facing growing levels of fraud, especially AI-driven fraud, use liveness detection to prevent fraud attacks on biometric systems from succeeding by ensuring that the person submitting a selfie is real, physically present, and not presenting a disguise.

Enhancing security

Face liveness detection enhances the security of digital interactions and transactions by detecting spoofing attempts. It adds an extra layer of protection against advanced spoofing techniques.

Removing friction

The latest face liveness detection methods, especially passive and hybrid approaches, offer a smooth and non-intrusive verification process, making liveness checks convenient for users and meeting the need for frictionless digital interactions.

Improving accuracy

Liveness detection improves the accuracy of biometric systems by differentiating between genuine and fraudulent biometric data.

Key sectors

Because face liveness detection is a key component of face biometric-driven identity verification, authentication, and assurance, the key sectors that are adopting the technology are predominantly those that are high-assurance, often highly regulated.

Biometric Intelligence has identified seven key sectors that are leading the way with adoption of face liveness detection:

1. Financial Services
2. Government
3. Enterprise
4. Gaming / Gambling
5. eCommerce / Retail
6. Healthcare
7. Travel (includes border control)

Financial services

AML / KYC regulation is an important driver for the use of face liveness detection in financial services.

Identity-related fraud is also a growing concern for the financial services sector, driven by the malicious use of AI including deepfake attacks on face biometric systems.

A September, 2024 Medius study found that 87 percent of finance professionals admit they would make a payment if 'called' by their CEO/CFO, and 53 percent have already experienced attempted deepfake scam attacks.

Face liveness detection has become a critical tool to detect and deter identity and financial fraud.

Government

Governments are accelerating digital transformation programs and this comes with risk.

The need to accurately identify citizens accessing digital government services is a vital part of delivering secure digital government services, and the need to know that it is a real person accessing them is becoming increasingly necessary.

This is especially important for tax and welfare services and when applying for or renewing government-issued identity documents including driver's licenses, national ID, and passports.

Enterprise

The adoption use-cases of Microsoft leveraging face biometrics and liveness capabilities for its Entra cloud-based identity and access management solution and LinkedIn partnering with IDV specialist Persona for its verified identity capability detail the importance of face liveness detection for enterprise digital technology and infrastructure. Enterprise workers using Microsoft Entra ID can also use iProov biometrics and liveness detection to log into company systems through Windows login, and to shared terminals, corporate assets via browsers for remote work, and to enter secure buildings.

The ability to prove identity and personhood is now an integral part of a modern digital workplace supporting a range of enterprise applications including:

1. Onboarding employees: especially important for remote working scenarios.

2. Privileged access control: linked to privileged identity and access management (PIM/PAM).

3. Fraud detection in web conferences: proving identity and personhood in business web calls.

4. Remote worker authentication: reducing home and remote working fraud where an imposter or alternative worker attempts to gain access to business digital services.

Gaming / Gambling

To counteract fraud and to support proof of age (age assurance) requirements, the gaming and gambling communities are turning to face liveness detection in increasing numbers.

The ability to prove identity and personhood, support secure onboarding and reduce money laundering liabilities through liveness detection is an important countermeasure to fraud in a sector that has historical problems with organized crime.

eCommerce / Retail

Face liveness detection is being used increasingly for both digital (eCommerce) and physical (in-store) commerce scenarios.

Popular applications include digital onboarding, payment security, and face age assurance (estimation).

Governments are increasingly using legislation to prevent young people from accessing restricted goods and services, including alcohol, medication, and dangerous weapons including knives and drugs, and age or identity assurance with liveness detection enables regulatory compliance.

Healthcare

Healthcare providers around the world lose billions of dollars in fraud. The UK's NHS lost £7.5 billion (roughly $9.3 billion) to fraud in the six years to 2023.

The FBI lists the following health care fraud types as common and identity-related.

1. **Identity theft/identity swapping:** Using another person's health insurance or allowing another person to use your insurance.
2. **Impersonating a healthcare professional:** Providing or billing for health services or equipment without a license.

Combining identity proofing and verification with face liveness detection can be a crucial tool in preventing healthcare fraud.

Travel

The travel industry is a beacon of light for the adoption of portable digital identity, backed by global standards and using government-grade security.

Remote digital services are transforming the travel industry, enabling passengers to book tickets, prove their identity with government-issued documents, including passports, check-in to flights, all from the comfort of their home or office – before they leave to travel.

On the day of travel, face biometrics and liveness detection are being leveraged to ensure that passengers have a safe and smooth transition through the travel hub and onto their plane, train, or boat.

Key Applications

We have identified four key applications that face liveness detection is enabling or supporting. The four are:

1. Digital Onboarding

2. Biometric Authentication

3. Document Authentication

4. Account Management

Digital onboarding

Digital onboarding is the process of using technology to integrate new customers or employees into a service or organization. It is often called identity proofing or identity verification.

Biometrics is a vital tool for remote customer onboarding for a wide range of sectors, with particularly high adoption in financial services.

Face liveness detection is a critical component for digital onboarding that prevents spoof attacks, ensuring that the applicant is a real person.

Identity verification and identity proofing are closely related but serve different purposes in the process of confirming someone's identity.

Identity proofing is the initial step, and is carried out to **validate** that a person is who they claim to be. This involves collecting and analyzing personal data and documents. It includes gathering information such as name, date of birth, and address, and verifying identity documents like passports or driving licenses. Often, biometric data (like fingerprints or facial recognition) is also used. The result of identity proofing is a validated identity that can be used for further verification steps.

Identity verification is the subsequent step that **confirms** the authenticity of the information and documents provided during the identity proofing stage. It can involve checking the

validity of the documents and data collected. Methods can include comparing photographs on identity documents, validating biometric data, or verifying addresses and phone numbers.

Adoption of biometric onboarding services has been strong, driven by a combination of AML/KYC compliance, fraud reduction and digital transformation programs across sectors pushing onboarding to the home through remote, unattended, means.

Biometric authentication

Biometric authentication is a security process that uses an individual's unique physical or behavioral characteristics to assert and verify their identity, comparing the presented biometrics to a stored version (template).

For the purposes of this study, the biometric modality is face.

Face liveness detection enhances face biometric authentication by ensuring that the presented face is a real person. When face liveness detection is used, the biometric authentication process includes matching the presented face with the template and verifying that it is a living, real person.

If active face liveness is used, then the person will be requested to speak, move their head from side-to-head, or blink their eyes.

For passive face liveness detection, the person will not be required to do anything additional. It will be part of the normal face biometric authentication process.

There is a movement within the industry away from using active face liveness detection to passive methods to ensure that the process is as smooth and frictionless as possible.

Document authentication

AI is being used for biometric authentication and liveness detection. It is also being used to support another important component of identity verification, document authentication.

Ensuring that a government-issued identity document is real, not a fake or has not been tampered with is an essential process in identity verification. The most common form of identity document tampering is portrait substitution, replacing the holder's image.

According to ID R&D, 70 percent of fraud in digital onboarding and KYC is with document fraud. To combat this attack, ID R&D has developed document liveness detection software that detects when an identity document is not genuine but instead a document presentation attack.

Liveness detection can be used to verify documents during onboarding.

Account management

Account management is often an overlooked area of digital service delivery, one that it is critical to cybersecurity health and hygiene.

If a fraudster successfully resets a password, they can then have full access to a person's account and commit many types of fraud, including draining a victim's bank account.

In the UK, password reset scams occur every seven minutes – that's 70,000 attacks per week -- and instances of password reset scams have risen by 421 percent between 2022 and 2023.

Ensuring that it is a real person requesting a password reset or new device setup is an important aspect of account management. Face liveness detection can be integrated into important aspects of account management where the risk of fraud is present, and we believe that this will be an important adoption area for the technology from 2025 onwards.

Detection Adoption

This section investigates adoption of face liveness detection on a regional basis, identifying key suppliers and sector focus.

It is a guide to adoption levels and reflects the health of a technology product or service.

Past and current adoption examples and levels are a key indicator for forecasting and form part of the quantitative data for forecasts.

This report includes four examples of liveness detection adoption from around the world. There are many more examples indicating an extremely healthy, and growing, technology sector.

Asia

Innovatrics and Govt of Thailand

The Government of Thailand has turned to Innovatrics to provide face liveness detection for the ThaiID mobile app.

In a bid to advance Thailand's digital infrastructure, the Digital Onboarding Toolkit (DOT) powered by Innovatrics' ABIS (automated biometric identification system) has been deployed as an extension of the existing National ID (NID) ecosystem to enable unsupervised identity verification from a smartphone. The move is intended to make the country's digital IDs safer and more secure to use.

The DOT components have been integrated into the government's ThaiID mobile app, and are used for remote onboarding with biometric identity checks being performed in the government data center, a recent case study reveals. The adoption of remote identity verification introduced the need for biometric liveness detection and optical character recognition (OCR) to read the Thai NID card.

Europe – UK

Mitek ID R&D and Virgin Money

Virgin Money turned to ID R&D to help prevent fraud and to counteract AI-Driven identity fraud.

Virgin Money serves more than six million customers across the UK and is a digital-first bank.

Virgin (now owned by the Nationwide Building Society) implemented digital identity checks to verify customer identities. Two of the identity verification processes the bank employs are facial recognition and selfie capture, which compare selfies at login to selfies on file to prevent fraud.

However, fraudsters and their methods are becoming more sophisticated, using deepfakes and even 3D masks to fool facial recognition technology. To get ahead of the current wave of fraudulent attempts, Virgin uses ID R&D liveness detection technology.

North America – USA

FaceTec and Civic

On-chain digital ID service provider Civic announced Proof of Personhood for decentralized apps (or "dApps") partnering with face and liveness specialist FaceTec, building on Solana to verify user's identities, screen out AI, and protect their services from abuse.

Proof of Personhood establishes that an individual digital wallet belongs to a unique human. First, a wallet owner proves their personhood by taking a live video selfie. The owner biometrically re-authenticates from time to time, again using FaceTec's liveness detection, to prove that the wallet has not been taken over by an AI agent or bot at a later point.

Proof of Personhood, as well as all Civic Passes, are 'soulbound' tokens that are issued and added to a user's wallet after their credentials have been verified.

The Proof of Personhood feature was designed for organizations to suppress trading bots, stop Sybil attacks, and to conduct secure decentralized autonomous organization voting. It can also be used to ensure online communities consist of actual humans.

Civic Passes can be managed on Civic.me, the provider's identity management platform. Users can also add and link wallets to their digital identity using the platform.

North America – USA

NEC and MLB

Major League Baseball began offering an expedited stadium access service known as "Go-Ahead Entry" through the MLB Ballpark app in 2023, and has been steadily expanding it to venues across North America.

NEC provides liveness detection for the service, which allows fans to register a live selfie on the app, and then enter the stadium on game day without showing a ticket or scanning their phone.

NEC has long been among the leading developers of facial recognition, and was the first Japanese provider of liveness detection to be confirmed for compliance to ISO 30107.

MLB says "Go-Ahead Entry" is being gradually introduced at all 30 big-league baseball stadiums in Canada and the USA.

North America – USA

Paravision and HID

Global access control provider HID selected Paravision's face liveness detection to secure its enterprise-grade solutions for the retail, banking, air travel and healthcare sectors.

Liveness detection enables biometric physical access control systems to screen out spoof attempts and detect people attempting to impersonate authorized customers or personnel to gain access to private or secure areas.

Paravision software has been integrated with HID's U.ARE.U 3D camera system, ArcID Biometric Server and DigitalPersona Biometric SDKs.

USA-based HID, a subsidiary of Sweden's Assa Abloy, chose Paravision's liveness as a way to achieve high security while complying with the privacy protection requirements of the EU's GDPR.

South America – Brazil

Unico and Oz Forensics

Unico acquired Oz Forensics in September 2024 and has integrated its proprietary liveness detection software into its digital identity and biometric authentication technology.

Oz Forensics offers face biometric, liveness and deepfake detection solutions. The face liveness technology has a 97 percent conversion rate in the first attempt and zero FAR (False Acceptance Rate).

Oz Forensics liveness detection is used by Unico's authentication technology, boosting it to a claimed 99.7 percent conversion rate.

Unico is an identity and facial biometrics platform, which through its neural network simultaneously operates three of the largest biometrics engines in the world, offering solutions for fraud prevention, access identification, and cost reduction.

Unico carries out biometric identification to confirm a customer's identity on behalf of different service providers. Due to the pandemic, the demand for remote identity verification has significantly increased, and so has the frequency of identity fraud. As a result, Unico decided to enhance its existing digital onboarding system. The solution needed to provide more efficient online identity verification with a frictionless user journey.

Unico's acquisition of Oz Forensics ensures that the digital identity provider owns the liveness components of their end-to-end identity solution.

"The partnership with Oz has undoubtedly strengthened our solution and improved reliability. For a major player like Unico, obtaining a trustworthy, agile, and secure solution is essential, and Oz proved to be the right choice for us", Diego Poblete, Head of Product at Unico.

South America – Brazil

iProov and Caf

UK-based face biometrics and liveness supplier, iProov, has entered into a strategic partnership with Caf, a supplier in the digital identity sector, that will enable businesses across Brazil to combat the rampant growth of identity-related fraud.

The partnership integrates iProov's facial biometric liveness technology into Caf's Know Your Everything platform. The majority of Caf's customer base, including banks, retailers, marketplaces, and fintechs have already adopted the iProov solution.

Fraud in Brazil is at an all-time high as criminals exploit the country's large population and high internet and mobile phone usage. Data from Brazil's central bank for the first quarter of 2023 found there were 2,800 financial fraud attempts per minute in digital channels equating to 365 million fraud attempts. Caf's own study for the same period shows that 1.73 percent of digital transactions in the country's financial system had criminal intent. A report by the Brazilian Banking Federation found that digital fraud accounted for 60 percent of all fraud losses in Brazil, seeing almost one in three Brazilians fall victim to financial scams and fraud.

In a separate announcement from iProov in 2024, the company revealed it is providing its face liveness detection to Microsoft Entra to secure workforce IDs. iProov's face biometrics and liveness can be added to Microsoft Entra deployments without complex integration to streamline onboarding and improve user experiences for employees with single sign-on (SSO) and passwordless logins. Faster and more secure access to company resources also improves productivity, according to the announcement.

Face Liveness Market Forecasts

Introduction

Market forecasting is very important in the Goode Intelligence (GI) research and analysis methodology especially when dealing with new or emerging markets and products.

GI has an excellent track record of forecasting in emerging technology areas including correctly predicting the growth of the mobile as an authentication device in 2009, the emergence of biometrics on mobile devices in 2011, and the growth in digital identity in 2015.

Market forecasting is one of the tools that GI uses in predicting the degree of success a new product or service will enjoy in the marketplace. The GI methodology considers areas such as *product awareness*, *distribution*, *price*, *fulfilling unmet needs* and *competitive alternatives*.

GI creates forecasts by gathering data from diverse sources like company filings, economic reports, and direct interactions (interviews) with both suppliers and buyers, some of which are bound by NDAs. GI then applies both quantitative methods and qualitative assessments (such as expert opinions) within financial models. These models are designed to estimate future performance by incorporating macroeconomic factors, industry trends, and company-specific details to provide a comprehensive view of expected growth and profitability

Revenue forecasting at Goode Intelligence (GI) involves collecting data from a variety of sources such as company filings, economic reports, and interviews with suppliers and buyers, often under NDA. This

information feeds into financial models that use both quantitative and qualitative methods, including expert opinions, to project future performance. These models consider macroeconomic factors, industry trends, and company-specific details. For revenue projections, GI calculates an average price, taking into account the variability in vendor pricing and potential discounts. The result is a comprehensive estimate of expected revenue growth and profitability for new or emerging products and markets.

We always welcome feedback from readers on the accuracy of the forecasts and are open to reflecting your opinion in future reports.

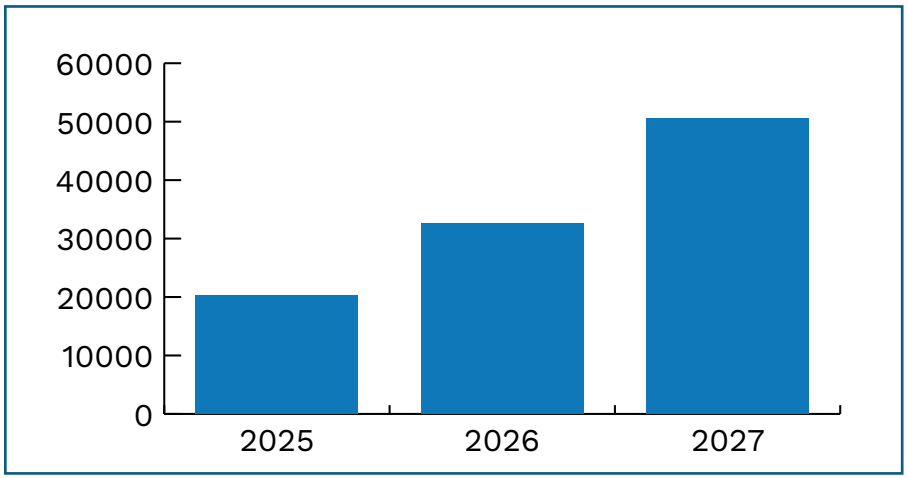
The forecasts consider a three-year forecast period, 2025-2027, covering:

1. Total Global Transactions
2. Total Global Revenue

Face Liveness Forecasts – Transactions

These forecasts are for total global face liveness transactions made annually.

Chart 1: Face Liveness Detection Forecasts: Total Global Transactions (m)



Source: Goode Intelligence © 2025

Table 1: Face Liveness Detection Forecasts: Total Global Transactions (m)

	2025	2026	2027
Total	20321.71	32670.09	50503.28

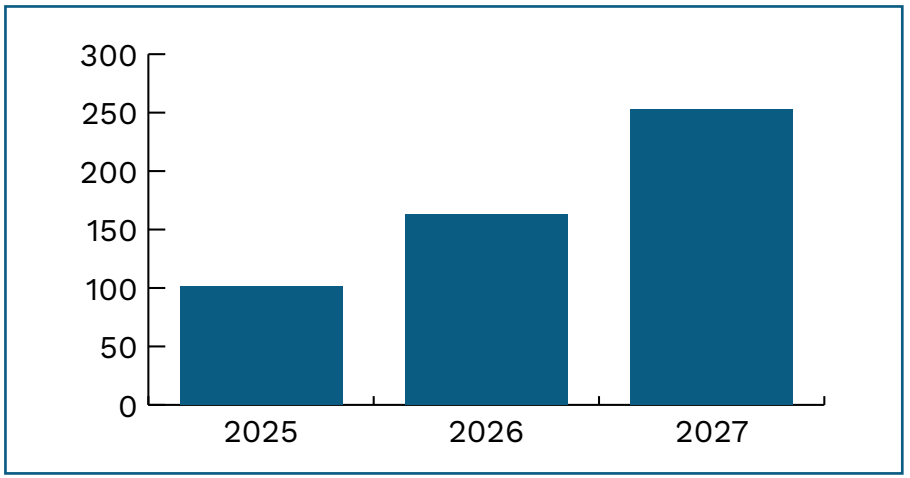
Source: Goode Intelligence © 2025

Face Liveness Detection Transactions will exceed 50 Billion Annually by 2027

Face Liveness Forecasts – Revenue

These forecasts are for total annual global face liveness revenue in US dollars (million).

Chart 2: Face Liveness Detection Forecasts: Total Global Revenue (m)



Source: Goode Intelligence © 2025

Table 1: Face Liveness Detection Forecasts: Total Global Revenue (m)

	2025	2026	2027
Total	101.61	163.35	252.52

Source: Goode Intelligence © 2025

Face Liveness Detection Revenue will exceed $252 million annually by 2027

Face Liveness Buyer's Guide

This guide provides potential buyers of face liveness products and services with information on how to assess solutions.

It is important to note that this guide should not be used as the sole method for assessing face liveness solutions as that is based on an organization's individual and specific requirements that should be included in a comprehensive assessment.

The buyers guide also includes a list of face liveness vendors (suppliers) that are active in the market. For a select number of vendors, there is a profile of the company and their products.

Biometric Update and Goode Intelligence strives to provide accurate information, but we must point out that our list of vendors is not comprehensive. We have selected a representative group of vendors, but we do not guarantee that our list is exhaustive. The analysis is presented on a "best efforts" basis, and we cannot accept any liability for any errors or omissions.

If a vendor considers that we have unreasonably omitted them then there is an opportunity for them to engage with Biometric Update and Goode Intelligence for inclusion in subsequent editions of this report.

What to look for in a face liveness detection supplier

This study provides a guide for buyers in what to look for in a face liveness detection supplier and identifies the following baseline criteria for measuring whether a face liveness detection is suitable:

1 **Cost - does it meet your budget expectations.** This is especially important when dealing with suppliers that charge per transaction, which is often the case. If you are entering into a per transaction contract, have you sized your requirements for now and for future growth and does your budget meet this?

2 **Accuracy and Reliability - is it a certified / tested product?** The main standards for testing liveness detection are the ISO/IEC 30107-3:2023 standard and certain FIDO certifications. This is considered to be "table stakes" when assessing whether a face liveness detection solution is effective.

3 **The Extra Mile - Does the supplier 'go beyond' ISO/IEC 30107-3:2023 and FIDO certifications?** Can the solution detect deepfakes and injection attacks, and what steps are being taken to detect and prevent the latest spoof attacks?

4 **Security** - does the supplier have cybersecurity certifications and adhere to cybersecurity guidance / best practice including offering a spoof bounty program?

5 **Does it meet your specific useability requirements?** The ability to fit in with your usability (UX) requirements is an important consideration when choosing a face liveness detection supplier. This includes whether a solution offers either active or passive liveness detection.

6 **Privacy and data protection compliance:** Does it meet EU GDPR and other state legislation related to the collection, storage and use of biometric data?

7 **Integration:** Check whether the solution can be easily integrated into existing systems and workflow.

What customers should ask liveness providers

The independent biometric testing labs also shared their experiences with us to shine a light on what customers should ask when evaluating liveness detection providers.

Ask how the system will adapt to emerging future threats, BixeLab advises.

Like other biometrics tests, liveness testing is largely about identifying and understanding risks, according to Ingenium. That means tested liveness providers should have a clear sense of what risks their system effectively defends against, and those risks that it doesn't.

Fime emphasizes the importance of ensuring performance in production, and that best practices are followed. Personal data acquired in the field could potentially be used for continuous algorithm improvement, for example, but this must be carried out in alignment with regulatory requirements and appropriate risk mitigation.

iBeta suggests inquiring about how the vendor self-polices for errors that slip through, and whether it has a routine system for updates to address those errors.

- **How often is the software updated?**
- **How is the data collected handled?**
- **How do you find weaknesses in the system?**

Vendor Profiles & Case Studies

Biometric Update and Goode Intelligence have identified more than 70 vendors that provide face liveness detection technologies. The technologies for face liveness detection are in many cases developed by companies that draw on extensive experience with user authentication and fraud prevention. In many cases, suppliers are experts in face biometrics, drawing on their extensive understanding of the underlying technology to prevent and detect presentation attacks. In many cases, face liveness detection solutions are used in combination with deepfake and injection attack detection solutions, often being bundled (aggregated) into a combined solution. The vendors profiled use a variety of techniques and offer software for a range of applications but are united by a mission to stop presentation attack fraud.

iProov

iproov.com
contact@iproov.com
10 York Rd, London SE1 7ND, United Kingdom
+44 20 7959 4373

iProov provides science-based biometric solutions that enable the world's most security-conscious organizations to streamline secure remote onboarding and authentication for digital and physical access. The company is committed to security and inclusivity by design, and boasts a list of certifications to prove it.

Based in London, UK, the firm's tools are trusted by organizations including the UK Home Office, U.S. Department of Homeland Security, NHS, the Australian Taxation Office, GovTech Singapore, UBS and Rabobank.

iProov Liveness is a fully-managed service that provides resilience against presentation, injection and deepfake attacks. It is a passive, multi-frame product optimized for inclusivity and security, and the only liveness product conformant to Web Content Accessibility Guidelines (WCAG) 2.2 Level AA, meeting the requirement for "Accessible Authentication."

The solution analyzes a range of signals from the user transaction, including the device metadata for signs of injection and the submitted imagery for signs of digitally-altered content. In addition, iProov operates threat monitoring on live traffic, leveraging machine learning models that look for patterns of attack.

The iProov Liveness SDK offers two options. Express Liveness is a near-instant multi-frame capture that verifies it's a real person in front of the camera. Dynamic Liveness adds a passive challenge response for higher assurance that the individual is genuinely present – the world's first FIDO-certified solution for remote face verification, accredited by Ingenium Biometrics.

Unlike active challenges, like a nod or a head turn, iProov doesn't require the user to follow any instructions. Instead, it uses patented Flashmark technology to illuminate the individual's face with a randomized sequence of colours. This color sequence is time-bound and verified to ensure the individual is authenticating in real time.

iProov Face Liveness has been independently tested by iBeta, a NIST-accredited biometrics lab, against ISO/IEC 30107-3:2017 standards for Presentation Attack Detection (PAD) Levels 1 and 2. In these tests, iBeta recorded a 0 percent success rate for all presentation attacks, including masks, photos, and other spoofs. Beyond that, iProov is extensively audited and tested for the highest levels of security and inclusivity, meeting SOC 2 Type II compliance and Section 508 requirements in the U.S. Rehabilitation Act requiring federal agencies to make their technology accessible to people with disabilities.

Jumio

www.jumio.com
marketing@jumio.com
100 Mathilda Place, Suite 100, Sunnyvale, CA 94086

Jumio helps organizations to know and trust their customers online. From account opening to ongoing monitoring, the Jumio Platform provides algorithmic identity intelligence anchored in biometric authentication, automation and data-driven insights, to accurately establish, maintain and reassert trust.

Leveraging powerful automated technology including biometric screening, AI/machine learning, liveness detection and no-code orchestration with hundreds of data sources, Jumio helps to fight fraud and financial crime, onboard customers faster and meet regulatory compliance including KYC and AML. Jumio has processed more than 1 billion transactions spanning over 200 countries and territories from real-time web and mobile transactions.

Based in Sunnyvale, California, Jumio operates globally with offices and representation in North America, Latin America, Europe, Asia Pacific, and the Middle East and has been the recipient of numerous awards for innovation.

Jumio says its liveness detection solution, Jumio Liveness, catches over 30 percent more sophisticated fraud attempts, without adding user friction. Customers maintain high conversion rates while reducing losses from advanced spoofing, including deepfakes and injection attacks. The latter have proven particularly damaging, as AI-generated faces, synthetic overlays and injection techniques are deployed at scale by bad actors offering fraud-as-a-service.

Jumio Liveness complies with the ISO/IEC 30107-3 Presentation Attack Detection (PAD) standard and is undergoing certification for Level 2 PAD. However, with its top tier offering, Jumio Liveness Premium, the company goes beyond ISO standards, detecting injection and replay attacks, forced verifications, unconscious individuals and multi-person attempts. Its tech stack includes an identity intelligence framework leveraging billions of processed transactions, and patented "active illumination" tech that combines randomized color sequences and AI-driven analysis to confirm human presence in real time, in order to stop sophisticated fraud, ensure compliance and build trusted relationships.

Mobai

mobai.bio
info@mobai.bio
Studievegen 16, 2815 Gjøvik, Norway
+47 242 00 002

Norway's Mobai provides AI-powered facial biometrics to combat identity fraud and deepfake threat, with a privacy-preserving approach that leverages patented, fully homomorphic encryption to ensure quantum-proof protection of biometric data. As the first company to deliver all of the biometrics sub components in the ETSI 119 461 requirements for biometric sub systems, it enables banks and digital identity providers across the Nordics to meet stringent AML/KYC requirements and streamline customer onboarding under eiDAS 1.0 and 2.0 regulations.

Founded in 2019 as a spin-off from the Norwegian Biometrics Laboratory at the Norwegian University of Science and Technology, Mobai now partners with EU agencies as well as major Nordic providers in eID, finance and cybersecurity, offering a complete biometrics ecosystem with all ETSI-compliant biometric components: face verification, liveness detection, injection attack detection, deepfake detection and morphing attack detection.

Designed to detect both 2D and 3D presentation attacks, Mobai's deep learning liveness detection product uses advanced AI models to secure biometric systems against spoofing. It provides instant checks from a single photo and video stream analysis, accurately verifying live users to prevent deepfakes, static image attacks and display attacks, as well as sophisticated silicone- and latex-mask attacks.

Mobai's Face Liveness and Presentation Attack Detection (PAD) technology has been independently tested and certified by the Swiss Center for Biometrics Research and Testing (SCBRT), a FIDO Alliance Accredited Biometrics Laboratory. The evaluation was performed under the ISO/IEC 30107-3 and ISO/IEC 19989-3 international standard, the industry's benchmark for biometric anti-spoofing. Its certified deepfake detection and injection attack detection capabilities have been independently evaluated in accordance with TS 18099: Biometric Data Injection Attack Detection (CEN standard), ensuring compliance with the latest international requirements.

With easy-to-integrate SDKs for iOS, Android and React Native, Mobai offers a flexibility to tailor the user experience from using 1 frame to videos, including fully customizable capture. The technology is available both on-premise and SaaS deployments, offered at a flexible pricing model that scales with usage.

Oz Forensics

ozforensics.com
Office 384, Saih Shuaib bldg 2 area,
DIC, Dubai UAE

Oz Forensics is a Dubai-based provider of solutions to protect against biometric attacks and deepfake fraud. Oz Liveness is its advanced liveness detection solution, verifying that a real, present human interacts with the system. Using machine-learning, it prevents the most sophisticated presentation and injection attacks, such as deepfakes. Fast, secure, and user-friendly, Oz Liveness ensures trusted digital onboarding and authentication across industries. It has worked with firms including Unico, Payme and Eurasian Bank.

Oz Liveness currently has 0 False Acceptance Rate on lab tests and on production environments in our clients. Data from one of its largest clients show improvements of over 30 percent in False Rejection Rates, while conversion rose by close to 10 percent. The same client also reports a 41 percent faster capture process after adoption of Oz Liveness, proving the solution was created for security, but designed for high speeds.

Oz Liveness is ISO 30107-3 certified, both Level 1 and Level 2, with tests run by NIST-approved labs. The company continuously seeks third-party re-certifications, with its most recent round of lab tests conducted at BixeLab in Australia.

The compliance test, which consisted of more than 600 presentation attacks, was performed with Oz Forensics SDK versions 8.16.2 for iOS and 8.17.0 for Android and SDK Web version 1.7.12, and confirmed the technology's robustness in spoof detection across mobile and web browser environments. It provided Oz with certifications of Injection Attack Detection, in compliance with CEN/TS 18099, on Web, iOS and Android platforms. Oz Liveness had 100 percent coverage against these attacks, not only for Presentation Attack Detection (PAD) but also Injection Attack Detection (IAD).

Oz Forensics maintains continuous R&D against deepfakes, injection and PAD attacks. It offers a solution that is nimble in allowing for quick model updates, to stay on top of the most recent fraud attempts the market is facing. The firm's experience with clients in countries such as Brazil, Colombia, the Middle East and Asia has exposed it to a wide swath of attacks at varying levels of sophistication, providing a unique perspective and capability for protecting clients ahead of market threats.

Both passive and active liveness are available with Oz Liveness. Passive liveness has a multi-frame capture characteristic that makes it ideal for clients looking for optimum user experience with no security trade-offs.

Unico and Oz Forensics: a trusted partnership against identity fraud

Unico partnered with Oz Forensics to strengthen its fight against digital identity fraud. The collaboration focused on delivering secure, fast, and intuitive liveness technology that could scale with the needs of Latin America's largest identity provider.

According to **Mayra Barbosa, Product Manager at Unico**, the integration was remarkably simple and user-friendly, enabling her team to implement the solution without friction. "The liveness check is intuitive for end users and effortless to integrate," she noted.

The results were immediate and measurable. Unico saw a **conversion rate increase from 95.8% to 98.7%**, reflecting a substantial boost in performance and efficiency. Capture processes became significantly faster and more agile, minimizing drop-offs and enhancing user experience.

One of the most remarkable outcomes was the impact on senior users. Unico reported a **70% increase in successful conversions for users over 60**, proving that the solution is inclusive and adaptable across demographics.

Support was another differentiator. Barbosa emphasized that the assistance received from Oz Forensics was **fast, reliable, and tailored to companies managing high transaction volumes**. This responsiveness allowed Unico to maintain operational excellence while deploying at scale.

By combining Unico's market leadership with Oz Forensics' advanced biometric verification, the partnership delivered a seamless, secure, and scalable solution against identity fraud.

Trusted by Latin America's largest KYC provider.

Paravision

paravision.ai
info@paravision.ai
San Francisco, California

Paravision builds trusted Identity AI building blocks for face recognition, liveness, deepfake detection and age estimation. Based in San Francisco, California, it delivers high-performance, ethically-developed AI software used globally for identity, security and authentication, running seamlessly across cloud, edge and embedded environments. Paravision consistently performs well in global benchmarks across a wide range of use cases and demographic groups, including those from the National Institute of Standards and Technology (NIST), which recently ranked Paravision's software among the most accurate in the world for both authentication and identification.

Its liveness detection product, Paravision Liveness, is a passive, AI-powered technology that distinguishes between real users and presentation attacks without the need for prompts, gestures, or environmental aspects such as blinking lights. It prevents spoofing from photos, videos and 3D masks while ensuring seamless user experiences. Available via SDKs, APIs or containers, it integrates easily into existing identity verification and authentication workflows, and is deployable on cloud, edge, mobile or hybrid solutions, depending on customer needs. Paravision's newest version, Liveness 2.0 delivers breakthrough performance with a more than 90 percent reduction in error rates (BPCER @ APCER) across all key testing thresholds and more than 40 percent reduction in Failure to Acquire rates.

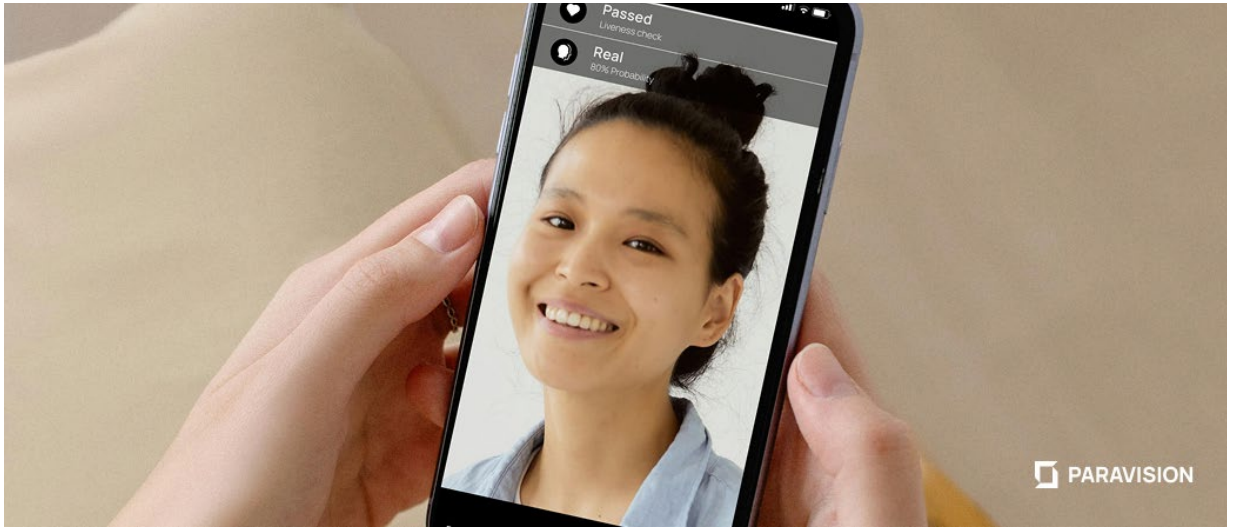
The product has been independently certified by iBeta to ISO/IEC 30107-3 standards for Level 1 and Level 2 Presentation Attack Detection. In addition, it has passed a Level 3 PAD evaluation by Ingenium, an ISO/IEC 17025-accredited test facility.

Beyond PAD, Paravision Liveness integrates with Paravision Deepfake Detection, enabling protection against emerging fraud vectors such as AI-generated media. This multi-layered approach ensures readiness against evolving spoofing and synthetic identity techniques. It also integrates seamlessly with Paravision Face Recognition and Age Estimation, giving organizations the building blocks for scalable, fraud-resistant, and inclusive digital identity systems.

Paravision Liveness is licensed by governments, major sports venues, travel hubs, financial services and leading identity verification providers around the world, and integrated into large-scale access control and security systems, travel solutions, and consumer digital onboarding workflows. Paravision has public partnerships with Entrust, HID, Checkin.com, ID.me, SITA, Secunet, Toppan Next Tech, AiFi, eConnect, PopID, Vicon, and Imprivata, among others.

Passive Liveness Redefines Secure, Seamless Identity Verification

Paravision Liveness is a fully passive solution that verifies real user presence without prompts or gestures. Designed to stop spoofing attempts using physical presentation attacks, including photos, videos, or 3D masks, Paravision Liveness delivers a seamless experience while maintaining the highest levels of security.



Independent evaluations have confirmed this balance of usability and protection. In 2025, Paravision achieved full compliance in Ingenium Biometrics' Level 3 Presentation Attack Detection evaluation, widely regarded as one of the most rigorous global PAD tests. The solution resisted 1,900 spoofing attempts across 190 unique instruments while maintaining low error rates for genuine users.

In parallel, the U.S. Department of Homeland Security's Remote Identity Validation Technology Demonstration (RIVTD) found Paravision delivered the lowest combined error rate—with APCER of 3.3% and BPCER of 0.3%—and the fastest processing time, averaging under one second. DHS RIVTD found that while both active and passive PAD systems were effective in detecting fraud, active systems proved to be significantly less convenient due to their much slower processing speeds.

Beyond certification, Paravision's newest release, Liveness 2.0, introduces a >90% reduction in error rates (BPCER @ APCER) across all key testing thresholds and >40% reduction in Failure to Acquire rates, and 2x faster speed on TensorRT compared to previous versions. With deployment options across SDKs, APIs, and containers, Liveness 2.0 is designed to integrate seamlessly with Paravision Face Recognition, Deepfake Detection, and Age Estimation, giving organizations the building blocks for scalable, fraud-resistant, and inclusive digital identity systems.

RealSense

https://realsenseai.com/
realsense@realsensai.com
20400 Stevens Creek Boulevard, Suite 290
Cupertino, CA 95014

RealSense ID is an award-winning, NIST-verified compact on-device facial authentication solution, built on a legacy of innovation in vision technology and AI. Incubated at Intel and purpose-built for user privacy and protection, RealSense ID combines an active depth sensor with a specialized neural network to deliver secure, accurate facial authentication.

RealSense ID is deployed via OEMs/integrators across enterprise access control, workforce management, healthcare, transportation, stadiums, retail, and kiosks/ATMs, and is optimized for high-traffic edge environments. This includes Ones Technology's BioAffix Gate Vision and BioAffix Mobile Gate Vision powered by RealSense ID F450—SIA NPS award winners (2024 Biometrics; 2025 Mobile Solutions). Other deployments include TabletKiosk, Farm Health Guardian, and select airports in Turkey and Israel. Separately, RealSense collaborates with NVIDIA on robotics initiatives and recently announced a strategic investment and partnership with dormakaba, a global leader in access solutions.

RealSense ID's anti-spoofing, liveness detection and facial authentication software achieves a 1 in a million false acceptance rate and a true-positive rate of 99.87 percent, unlocking in a fraction of a second. Active-stereo depth plus neural models analyze texture, micro-motion, and reflectance to block photos, videos, and masks without no prompts. Engineered to operate entirely on-device, the product eliminates the need to transmit biometric data to external servers, enhancing privacy and data security.

The specialized neural network reliably supports every skin tone and shade and adapts to changes over time, accommodating different hairstyles, facial hair and more. It functions in conditions from complete darkness to bright sunlight, and its large vertical field of view means it can authenticate people from 120 cm to 190 cm tall at a 55 cm distance.

RealSense ID is currently undergoing ISO/IEC 30107-3 (Presentation Attack Detection) evaluation under iBeta Quality Assurance. It has achieved Google's PAD Certification in Spain through IOActive. Its models, user database, and operational firmware are encrypted (AES-256) and digitally signed (ECDSA-256); only authenticated components run, and updates are verified before install. Matching runs on-device, keeping biometric data off external servers.

RealSense ID is priced per device, and comes with no cloud or per-transaction fees.

Regula

regulaforensics.com
info.lv@regulaforensics.com
34 Višķu Street, Daugavpils, LV-5410
+371 65 43 12 99

Regula, a global leader in forensic devices and identity verification, leverages more than 30 years of expertise and the world's largest document template library to deliver breakthrough biometric technologies.

Based in Daugavpils, Latvia, the firm is trusted by over 1,000 organizations, with customers in banking, fintech, telecom, aviation, hospitality, KYC and identity verification, plus 80 border control authorities. Regula's tools successfully perform up to one billion verifications a year in over 250 countries and territories.

The company's proprietary liveness detection technology streamlines remote biometric verification and efficiently prevents fraudulent presentation attacks, such as the use of static face images with electronic devices, printed photos, video replays, video injections, or realistic 3D silicon masks. It combines factors like texture analysis, image depth and facial movement to determine whether a person is real or a fake representation.

The product instantly determines spoofing attacks with live face substitutes while verifying identity through a smartphone camera or desktop device. For PAD, Regula's internal testing shows a 0 percent False Acceptance Rate (FAR) / 5 percent False Rejection Rate (FRR).

Regula's document liveness detection technology verifies the presence of dynamic security features in the document, such as holograms, OVI, MLI, and Dynaprint. The solution offers facial recognition with both active and passive liveness detection techniques to effectively identify deepfakes, screenshots, video replays, injections, webcam hacks and more.

In compliance with global security standards, Regula Face SDK has successfully passed iBeta's PAD Level 1 and Level 2 tests according to ISO/IEC 30107-3. But its products create a complete framework for comprehensive identity verification across multiple layers. By adding signal integrity control that verifies the source of biometric and document data, Regula ensures attackers can't slip in manipulated inputs through injections or emulators.

Regula recently began participating in the NIST evaluation for facial age estimation. In the August 29, 2025 evaluation, the company outperformed all other vendors in many metrics. Crucially, Regula's technology demonstrated consistent accuracy across a wide range of demographics. Regula also ranked among the top three in two critical age assurance scenarios: Challenge 25 and Child Online Safety (ages 13–16) (as measured by mean absolute errors).

Youverse

youverse.id
sales@youverse.id
Taguspark, Núcleo Central, 147, 2740-122
Oeiras, Lisbon, Portugal

Youverse is built on a privacy-first, decentralized biometric engine, enabling businesses to meet compliance needs while protecting customers' data. From identity checks to authentication and age verification, processes become instantaneous, slashing onboarding time, easing compliance and blocking fraud. The EU-based company believes that a growing volume of data breaches and deepfake attacks shows the need for fintech, gaming, mobility and digital platform businesses to pivot to decentralized authentication with certified liveness for robust fraud prevention.

Youverse Face Liveness detects whether a face is real and present during verification. It protects against spoofing, deepfakes and injection attacks through AI-powered passive and active checks. A hybrid approach combines frictionless checks requiring no user action with active challenges when additional assurance is needed. This balances user experience and security, adapting dynamically to threat levels and ensuring resilience against advanced spoofing and injection attacks.

Face Liveness consistently delivers high reliability, with independent tests by certified entities such as iBeta confirming robust performance across devices, environments and attack types, ensuring strong protection against spoofing while maintaining a smooth user experience. The API is stress-tested against diverse real-world conditions, including low light, device variability, and complex spoofing attempts.

Beyond ISO/FIDO compliance, Youverse continuously enhances resilience to emerging threats. Its models detect presentation attacks, synthetic media (deepfakes, face swaps) and injection attacks (bypassing camera feeds), and were designed to conform to the recent ETSI standard CEN/TS 18099:2024.

Youverse's Face Liveness adds negligible latency (typically less than 1 second) and minimal incremental cost to IDV flows, while significantly reducing fraud-related losses. It works on a usage-based pricing model to ensure predictable scaling without prohibitive overheads. Delivered via flexible API/SDK, it integrates seamlessly with existing IDV and authentication flows.

Face Liveness Vendors Directory

1

1Kosmos

1kosmos.com

1Kosmos is a private company founded in 2017 and headquartered in East Brunswick, New Jersey, USA. The company specializes in digital identity proofing and passwordless authentication solutions, combining advanced biometrics with blockchain technology.

1Kosmos integrates liveness detection into its biometric authentication solutions to ensure that the individual attempting to authenticate is physically present and not using fraudulent methods such as photos, videos, or deepfakes.

A

Accura Scan

accurascan.com

Accura Scan is a private company founded in 2017 and headquartered in Mumbai, Maharashtra, India. The company specializes in digital identity verification and KYC solutions, offering services such as OCR, facial biometrics, liveness detection, and AML screening.

These solutions cater to various industries, including banking, finance, telecommunications, and immigration, enabling secure and efficient customer onboarding and authentication processes.

Advance.AI

advance.ai

Advance.AI is a private company founded in 2016 and headquartered in Singapore. Its services include digital identity verification, compliance, fraud detection, and process automation, catering to industries such as banking, financial services, fintech, payment, retail, and e-commerce.

Advance.AI offers robust liveness detection technology to verify that an online user is a real person, effectively distinguishing between live images and fraudulent attempts such as 2D prints or video clips.

Alice Biometrics

alicebiometrics.com

Alice Biometrics is a private company founded in 2019 and headquartered in Spain. The company specializes in biometric identity verification solutions, offering services such as facial recognition, passive liveness detection, and automatic document reading.

These solutions facilitate 100% online client onboarding, ensuring compliance with KYC and AML regulations, thereby increasing conversion rates and minimizing fraud.

AU10TIX

au10tix.com

AU10TIX is a private company founded in 2002 and headquartered in Israel. The company specializes in identity verification and risk management solutions, providing automated services for ID document authentication and fraud detection.

AU10TIX integrates liveness detection into its biometric verification solutions to ensure that the individual being

authenticated is physically present and not using fraudulent methods such as photos, videos, or masks.

Authenticalls

authenticalls.com

Authenticalls, founded in 2022, is headquartered in Dublin, Ireland with an additional location in Zug, Switzerland. The company specializes in enhancing digital security through advanced identity verification solutions, focusing on authentication and document verification.

Authenticalls employs biometric KYC with liveness face matching to ensure that the individual undergoing verification is physically present. This process involves automated data reading and matching, reducing human error and operational costs.

authID

authid.ai

authID Inc., formerly known as Ipsidy Inc., was founded in 2009 and is headquartered in Denver, Colorado, USA. The company specializes in providing secure, biometric identity verification and passwordless authentication solutions for both consumer and workforce applications worldwide.

authID.ai integrates liveness detection into its biometric authentication solutions to ensure that the individual being authenticated is physically present and not using fraudulent methods such as photos, videos, or deepfakes.

AuthMe

authme.com

Authme is a private company founded in 2019 and is headquartered in Taipei City, Taiwan. Authme specializes in digital identity verification solutions, offering services such as ID document verification, facial recognition, and liveness detection.

Its AI-powered platform enhances security and efficiency for businesses by simplifying the KYC process and protecting against identity fraud.

Aware

aware.com

Aware, Inc. is a publicly traded company founded in 1986 and headquartered in Burlington, Massachusetts, USA. The company specializes in biometrics software products and solutions, providing authentication services for government agencies and commercial entities worldwide.

Aware integrates liveness detection into its biometric authentication solutions which cater to various industries including financial services, healthcare, law enforcement, and border management, enabling secure identity verification and management.

AWS (Rekognition)

aws.amazon.com

Amazon is a public company headquartered in Seattle, Washington, USA. Amazon Web Services launched Amazon Rekognition Face Liveness in 2023 and now available in five AWS regions - US East (N. Virginia), US West (Oregon), Europe (Ireland), Asia Pacific (Tokyo), and Asia Pacific (Mumbai).

Amazon Rekognition Face Liveness is a fully managed feature that can be integrated to apps running on most devices with a front-facing camera. The 'near-passive' software uses a short video, includes injection attack detection and has passed a Level 2 PAD evaluation by iBeta. It is used for user onboarding, step-up authentication, age verification and bot detection.

B

BioID

bioid.com

BioID GmbH is a private company founded in 1998, originating from a research project at the German research institute Fraunhofer IIS and headquartered in Nuremberg, Germany. BioID specializes in biometric authentication software, offering services such as facial recognition, certified liveness detection, and periocular recognition.

Its solutions cater to various industries, including financial services, healthcare, and government organizations, providing secure and convenient identity verification and authentication.

Biometriq

biometriq.pl

BiometrIQ, founded in 2019, is headquartered in Lublin, Poland. The company specializes in advanced biometric technologies, focusing on voice biometrics and liveness detection. Its services encompass research and development projects, consulting, and the implementation of biometric systems.

The company runs numerous research projects aiming at the development of new methods to fight fraudulent attacks in voice biometric systems. This includes ensuring that the individual providing a voice sample is physically present and not using recorded or synthesized voices. By incorporating these advanced liveness detection technologies, BiometrIQ enhances the security and reliability of its biometric systems, ensuring that only live, genuine individuals can successfully authenticate.

C

Chooch

chooch.com

Chooch AI is a private company founded in 2015 and is headquartered in San Mateo, California, USA. Chooch AI specializes in computer vision and artificial intelligence solutions, offering a platform that enables businesses and government agencies to deploy AI vision capabilities in the cloud, at the edge, or both.

The company integrates liveness detection into its facial authentication solutions

CyberLink

cyberlink.com

CyberLink Corp. is a publicly traded company founded in 1996 and is headquartered in New Taipei City, Taiwan. CyberLink specializes in multimedia software and AI facial recognition technology, offering a range of solutions for digital content creation, multimedia playback, video conferencing, live casting, mobile applications, and AI facial recognition.

CyberLink integrates liveness detection into its facial recognition platform.

D

Daltrey

daltrey.com

Daltrey, founded in 2001, is headquartered in Sydney, Australia. The company specializes in biometric cyber-defense, offering advanced authentication solutions that integrate seamlessly into existing security frameworks. Daltrey's mission is to eliminate weak credentials by providing strong, secure, and frictionless authentication across various access points, both digital and physical.

Daltrey incorporates liveness detection into its biometric solutions to ensure that the individual being authenticated is physically present. This prevents spoofing attempts using photos, videos, or masks, thereby enhancing security. Its liveness detection capabilities are designed to provide impersonation-resistant authentication, ensuring that only live, genuine individuals can successfully authenticate.

Daon

daon.com

Daon is a private company founded in 2000 and headquartered in Fairfax, Virginia, USA, with additional operations in Dublin, Ireland, and regional offices in Serbia and Australia. Daon specializes in biometric authentication and identity assurance solutions.

Daon integrates liveness detection into its biometric authentication solutions which are utilized across various industries including financial services, healthcare, public sector, retail, telecommunications, and travel, to provide secure and convenient identity verification and authentication services.

Dermalog

dermalog.com

DERMALOG Identification Systems GmbH is a private company founded in 1995 and headquartered in Hamburg, Germany, with additional offices in Malaysia and Singapore. DERMALOG specializes in biometric identification solutions, including Automated Fingerprint Identification Systems (AFIS), Automated Biometric Identification Systems (ABIS), and biometric devices such as fingerprint and document scanners.

DERMALOG integrates liveness detection into its biometric solutions which are utilized across various sectors including banking, public administration, and law enforcement, protecting the identities of millions of people in more than 100 countries.

Dojah

dojah.io

Dojah, founded in 2020, is headquartered in Lagos, Nigeria. The company specializes in fraud prevention and identity verification solutions, offering a comprehensive platform that enables businesses to securely onboard and authenticate users.

Dojah provides an AI-powered facial recognition technology that analyzes human expressions, such as smiling and blinking, to confirm the presence of a live user during the verification process. This method enhances security by preventing spoofing attempts using static images or videos. Dojah's liveness detection can be integrated via API, allowing businesses to incorporate this feature into their existing systems seamlessly.

E

Entrust

entrust.com

Entrust Corporation, formerly known as Entrust Datacard, was founded in 1969 as Data Card Addressograph and is headquartered in Shakopee, Minnesota, USA.

Entrust specializes in digital security solutions, including identity verification, secure payments, and data protection. Entrust integrates liveness detection into its biometric authentication solutions.

F

FaceOnLive

faceonlive.com

FaceOnLive, established in 2021, is headquartered in Oshawa, Ontario, Canada. The company specializes in on-premises identity verification and biometric authentication solutions, offering customizable software development kits (SDKs) to help businesses streamline customer onboarding while maintaining full control over their data.

One of its key products is Face Liveness Detection SDK, ensuring that the individual being verified is physically present, preventing spoofing attempts. FaceOnLive's solutions are designed to be fully customizable and on-premises, ensuring compliance with data privacy regulations such as GDPR, HIPAA, and CCPA.

Facephi

facephi.com

Facephi is a public company that was founded in 2012 and is headquartered in Alicante, Spain. Facephi specializes in digital identity protection and verification, noted for its focus on data security and integrity.

The company integrates liveness detection into its biometric identity verification solutions.

FaceTec

facetec.com

FaceTec is a private company founded in 2013 and is headquartered in Las Vegas, Nevada, USA. FaceTec specializes in 3D face authentication software, providing solutions for facial recognition and independently tested liveness detection.

Its technology is utilized across various industries, including financial services, border security, transportation, blockchain, e-voting, social networks, and online dating, enabling secure and reliable identity verification.

Facia.ai

facia.ai

Facia.ai is a private company founded in 2022 and is headquartered in London, UK. The company specializes in biometric authentication systems, offering AI-powered 3D facial recognition and liveness detection technology designed to identify and verify individuals worldwide.

Facia's platform helps prevent fraud and identity theft by protecting against spoofing attacks, including deepfakes, and is utilized across various industries such as banking and financial services, healthcare, government, and education.

Fourthline

fourthline.com

Fourthline, founded in 2013, is headquartered in Amsterdam, Netherlands. The company specializes in providing comprehensive identity verification and compliance solutions, primarily serving the financial sector, including banks, fintechs, and insurers.

Fourthline employs advanced techniques to ensure that individuals undergoing verification are physically present and actively participating. Their process involves clients submitting a selfie photo and performing a liveness check by turning their head left and right while a video is recorded. This method confirms that the client is a living person and not attempting to use fraudulent means such as photos, videos, or masks.

G

GET Group

getgroup.com

GET Group Holdings Ltd. is a private company with over 35 years of experience in identity management, security printing, and smart solutions and is headquartered in Dubai, UAE. GET Group provides identity management solutions including enrollment, secure document issuance, and digital identity systems.

GET Group offers proprietary facial liveness detection software as part of its biometric solutions. Notably, their solution has been tested and confirmed compliant with the ISO/IEC 30107-3 standard for presentation attack detection (PAD).

H

HID

hidglobal.com

HID Global Corporation was founded in 1991 and is headquartered in Austin, Texas, USA. The company specializes in secure identity products and services, including physical and logical access control, authentication and credential management, government ID solutions, and card printing and personalization. As a subsidiary of Assa Abloy, HID Global operates globally, serving various sectors such as government, financial services, corporate, education, and healthcare.

Hummingbirds AI

hummingbirds.ai

Hummingbirds AI is a private company founded in 2020 and is headquartered in Miami Beach, Florida, USA. The company specializes in bio-inspired vision AI technologies, focusing on enhancing security and user experience across various sectors.

Its flagship product, Guacamole is an AI-powered application that leverages facial matching to automate screen privacy and security.

I

ID R&D

idrnd.ai

ID R&D was founded in 2016 and is headquartered in New York City, New York, USA. In 2021, ID R&D was acquired by publicly traded Mitek Systems, a provider of digital identity verification solutions.

The company specializes in biometric authentication technologies, offering solutions such as voice and behavioral biometrics, voice anti-spoofing, and passive facial liveness detection. These technologies are designed to enhance security while providing a frictionless user experience across various industries, including finance, healthcare, and telecommunications.

IDcentral

idcentral.io

IDcentral, founded in 2019, is headquartered in Broomfield, Colorado, USA. The company specializes in cloud-based customer identification solutions aimed at fraud prevention. Its platform offers automated verification of identity cards and documents, catering to industries such as banking, telecommunications, retail, and insurance.

IDcentral provides both active and passive liveness checks to ensure that the individual undergoing verification is physically present. This technology helps prevent spoofing attempts using photos,

videos, or masks, enhancing security during the digital onboarding process.

Idemia

idemia.com

Idemia is a French multinational technology company headquartered in Courbevoie, Île-de-France, France. It was formed in 2017 through the merger of Oberthur Technologies and Safran Identity & Security (formerly known as Morpho).

Idemia specializes in identity-related security services, providing biometric identification products and software, including facial recognition systems, fingerprint and iris recognition, biometric terminals, e-gates, ID cards, ePassports, payment cards, and SIM cards.

Idemia's selfie liveness detection technology has successfully passed independent third-party testing for presentation attack detection (PAD) in accordance with ISO/IEC 30107-3 standards.

Idenfy

idenfy.com

iDenfy, founded in 2017, is headquartered in Kaunas, Lithuania. The company specializes in identity verification and fraud prevention solutions, assisting businesses in complying with KYC, AML, and KYB regulations.

iDenfy employs a patented 3D liveness detection technology to ensure that the individual undergoing verification is physically present. This technology instantly identifies fraudulent verification attempts, such as the use of photos, videos, or masks, by analyzing facial movements and depth. The system operates by matching the customer's live selfie biometrics with a reference image extracted from their ID document, utilizing AI-powered data extraction to confirm the face's authenticity.

Identomat

identomat.com

Identomat is a private company founded in 2019 and is headquartered in Champaign, Illinois, USA. Identomat specializes in AI-powered identity verification and KYC compliance solutions. Its platform offers services such as AML monitoring, biometric multi-factor authentication, account recovery, and video KYC with live multi-party video calls.

Identomat offers proprietary facial liveness detection software as part of its identity verification solutions. Its system includes both active and passive liveness checks to ensure the genuine presence of an individual during the verification process. These solutions cater to various industries, including banking and finance, healthcare, fintech, e-commerce, and government, enabling businesses to streamline customer onboarding and ensure compliance with regulatory requirements.

Identy.io

identy.io

Identy.io is a private firm founded in 2017 and is headquartered in Delaware, USA. It provides biometric authentication on mobile phones for identity verification in government sectors and the corporate landscape.

Face liveness and anti-spoofing mechanisms are supported through an extensive analysis of parameters extracted from the captured camera images. Identy.io's matcher has been

validated by NIST in its FRVT test and it complies with ISO 30107-3, levels 1 and 2, meeting global security regulations such as AML and GDPR, along with local financial and banking regulations.

IDnow

idnow.io

IDnow is a private company founded in 2014 and is headquartered in Munich, Germany, with additional offices in the United Kingdom and France.

IDnow specializes in identity verification-as-a-service, providing KYC and electronic signing solutions for various industries, including financial services, telecommunications, mobility, and travel. IDnow integrates liveness detection into its identity verification solutions.

Idology

idology.com

IDology is a private company founded in 2003 and is headquartered in Atlanta, Georgia, USA. The company specializes in digital identity verification and fraud prevention solutions, offering services such as data verification, document authentication, and biometric identification. In February 2019, IDology was acquired by GB Group plc (GBG), a global leader in digital identity and fraud prevention.

IDology offers proprietary facial liveness detection software as part of its identity verification solutions. Its Selfie ID Verification service integrates biometric facial recognition with passive liveness testing to confirm that the individual is physically present during the transaction. These solutions cater to various industries, including automotive, transportation, healthcare, insurance, and retail, enabling businesses to securely onboard customers, meet compliance regulations, and prevent fraud.

IDVerse

idverse.com

IDVerse, formerly known as OCR Labs Global, is a private company founded in 2014 and is headquartered in London, UK with additional offices in Sydney, Australia, and Silicon Valley, USA. IDVerse specializes in AI-powered identity verification solutions, offering services such as biometric verification, document fraud analysis, and face authentication. In December 2024, LexisNexis Risk Solutions announced a definitive agreement.

Using IDVerse's proprietary Liveness & Face Match technology, Face Access enables businesses to allow their end users to authenticate themselves within seconds by performing on-the-spot liveness capture and face match. to acquire IDVerse, aiming to enhance their digital identity capabilities.

iiDENTIFii

iidentifii.com

iiDENTIFii, founded in 2018, is headquartered in Cape Town, South Africa. The company specializes in biometric identity verification solutions, offering services including facial recognition, liveness detection, and document optical character recognition (OCR) for KYC and AML.

iiDENTIFii employs advanced techniques to confirm that the individual undergoing verification is physically present and not using fraudulent methods such as photos, videos, or masks. This process enhances security by preventing identity spoofing and ensuring that only live users can successfully authenticate.

Incode

incode.com

Incode Technologies Inc. is a private company founded in 2015 and is headquartered in San Francisco, California, USA. Incode specializes in AI-driven identity verification and authentication solutions. Its platform is utilized by industries including financial services, government, retail, hospitality, and healthcare, enabling customers to validate their identity using facial biometrics and government-issued IDs through web or mobile applications.

Incode's passive liveness technology accurately detects and prevents fraud by identifying physical spoofs like photo printouts and masks, as well as digital manipulations like AI-generated deepfakes, using advanced proprietary ML models and in-house AI.

Innovatrics

innovatrics.com

Innovatrics is a private company founded in 2004 and is headquartered in Bratislava, Slovakia. The company specializes in biometric solutions, offering products such as Automated Biometric Identification Systems (ABIS), digital onboarding toolkits, facial recognition platforms, and fingerprint and facial recognition algorithms.

These solutions cater to various sectors, including government, law enforcement, finance, and telecommunications, enabling secure and efficient identity verification and management. Innovatrics liveness detection can be fine-tuned to meet the requirements of a specific use case.

iProov

iProov.com

iProov provides science-based biometric solutions that enable the world's most security-conscious organizations to streamline secure remote onboarding and authentication for digital and physical access. The company is committed to security and inclusivity by design, and boasts a list of certifications to prove it.

Based in London, UK, the firm's tools are trusted by organizations including the UK Home Office, U.S. Department of Homeland Security, NHS, the Australian Taxation Office, GovTech Singapore, UBS and Rabobank.

J

Jumio

jumio.com

Jumio is a private company founded in 2010 and headquartered in Sunnyvale, California, USA. Jumio specializes in digital identity verification and authentication services, utilizing technologies such as artificial intelligence, biometrics, machine learning, and liveness detection.

Its solutions help organizations across various sectors, including financial services, digital currency, retail, travel, and online gaming, to onboard customers quickly, prevent fraud, and comply with regulatory requirements. Jumio Liveness increases the security of biometric systems and thwarts the well-documented vulnerabilities in less robust liveness technologies.

L

LexisNexis Risk Solutions

risk.lexisnexis.com

LexisNexis Risk Solutions, established in 1997, is headquartered in Alpharetta, Georgia, USA. It is a subsidiary of publicly traded firm RELX Group.

LexisNexis TrueID Document Authentication utilizes passive liveness detection and facial recognition matching algorithms to compare the photograph on an ID document with a selfie taken by the user. This process ensures that the individual is physically present during the authentication, enhancing security and reducing the risk of fraud.

M

Microsoft Azure AI Vision Face

microsoft.com

Microsoft, the global software giant headquartered in Redmond, Washington, was founded in 1975 and is one of the most valuable public U.S. companies. It creates platforms and tools powered by AI.

Microsoft announced the general availability of its face liveness detection features in January 2025 that is ISO/IEC 30107-3 iBeta level 1 and 2 compliant.

Megvii

megvii.com

Megvii is a private company founded in 2011 and headquartered in Beijing, China.

Megvii specializes in various applications of artificial intelligence, including liveness detection as part of its biometric and facial recognition solutions.

MiniAiLive

miniai.live

MiniAiLive Ltd. was incorporated in 2023 and specializes in touchless biometric authentication and identity verification solutions.

It offers advanced security technologies, including facial recognition, liveness detection, and ID document recognition, ensuring seamless integration with clients' existing systems.

Mobai

mobai.bio

Mobai, founded in 2019, is headquartered in Gjøvik, Norway. The company specializes in biometric face verification solutions, focusing on facial recognition, presentation attack detection, liveness detection, and morphing (deepfake) detection.

Its services are designed for identity verification and authentication for service providers in regulated markets, such as financial services.

N

NEC

nec.com

NEC Corporation was established in 1899 and is headquartered in Tokyo, Japan. NEC has developed advanced anti-spoofing technologies to enhance the security of its facial recognition systems.

Its liveness detection technology uses artificial intelligence to determine whether a subject is a real person or an inanimate representation, such as a photo, video, or mask. NEC's liveness

detection is suitable for various applications such as border control, access management, and secure transactions.

Neurotechnology

neurotechnology.com

Neurotechnology, founded in 1990, is headquartered in Vilnius, Lithuania and specializes in developing algorithms and software for biometric identification, computer vision, robotics, and artificial intelligence.

Neurotechnology has developed algorithms compliant with the ISO 30107-3 standard to prevent spoofing attempts, and these liveness detection capabilities are integrated into its facial recognition products.

NTechLab

ntechlab.com

NtechLab, established in 2015, is headquartered in Larnaca, Cyprus and specializes in advanced video analytics solutions powered by artificial intelligence, focusing on facial recognition, body detection, and vehicle identification.

NtechLab integrates liveness detection into its biometric user identification systems.

O

Onfido

onfido.com

Onfido, established in 2012, is headquartered in London, England and specializes in digital identity verification. It was acquired by Entrust Corporation in 2024.

Onfido employs advanced liveness detection techniques and is compliant with iBeta Level 2 standards, providing robust protection against sophisticated fraud.

OzForensics

ozforensics.com

Oz Forensics, founded in 2017, is headquartered in Dubai, United Arab Emirates and was acquired by Unico, a Brazilian ID company, in September 2024.

Oz Forensics specializes in biometric and deepfake identity fraud prevention, offering solutions such as liveness detection and biometric verification to both private and public organizations globally.

P

Paravision

paravision.ai

Paravision, founded in 2013, is headquartered in San Francisco, California and specializes in advanced computer vision technology, focusing on facial recognition, liveness detection, deepfake detection, and age estimation.

Paravision has developed advanced technology to confirm user authenticity by detecting spoofs using a standard selfie. Its offerings are utilized across various sectors, including digital identity verification, government programs, travel and border security, stadiums and events, automotive, payments and retail, and physical security.

Persona

withpersona.com

Founded in 2018, Persona is headquartered in San Francisco and is available in 200+ countries and territories. Persona's verified identity

platform helps organizations balance fraud prevention, conversion, and compliance by giving them the tools to tailor identity verification to their specific needs, regions, and risk profiles.

Organizations can use Persona across every stage of the identity life cycle, from data collection to decisioning, and for any scenario: KYC, KYB, fraud, age verification, workforce authentication, and more. This flexibility allows teams to quickly adapt as new technologies, regulations, and use cases emerge.

R

Regula

regulaforensics.com

Regula, established in 1992, is headquartered in Daugavpils, Latvia and specializes in identity verification solutions and forensic devices, providing automated and reliable document examination and biometric verification tools.

Regula has developed proprietary liveness detection technology to enhance remote biometric verification and prevent fraudulent presentation attacks.

ROC

roc.ai

Rank One Computing (ROC), established in 2015, is headquartered in Denver, Colorado and specializes in developing advanced biometric and computer vision solutions, including facial recognition, fingerprint recognition, iris recognition, and object detection.

ROC offers a patented single-frame passive liveness detection technology designed to prevent spoofing and fraud during identity verification processes.

S

Seamfix

seamfix.com

Seamfix, founded in 2007, is headquartered in Lagos, Nigeria. The company specializes in software development, focusing on identity management, data collection, and KYC processes.

Seamfix offers a passive liveness engine designed to authenticate users and enhance biometric security. The company serves various industries, including telecommunications, government, construction, and financial institutions, by providing tailored solutions to meet specific sector needs.

Sensity

sensity.ai

Sensity AI, founded in 2018, is headquartered in Amsterdam, Netherlands. The company specializes in developing advanced cybersecurity technologies aimed at detecting and combating AI-generated threats, particularly deepfakes. Its platform offers comprehensive detection tools for videos, images, audio, and identities, serving sectors such as law enforcement, KYC vendors, social media platforms, and defense agencies.

Sensity AI addresses the challenges posed by deepfake technology in online identity verification. Its solutions are designed to identify AI-generated content that can compromise facial recognition and liveness checks, which are critical components of biometric identity verification systems. By detecting these sophisticated forgeries, Sensity AI enhances the security and reliability of identity verification processes, ensuring that only live, genuine individuals can successfully authenticate.

Smile ID

usesmileid.com

Smile ID, formerly known as Smile Identity, was founded in 2017. The company is headquartered in Lagos, Nigeria, with additional offices across five countries.

Smile ID specializes in digital identity verification, fraud detection, AML and KYC compliance solutions tailored for businesses operating in Africa. Its mission is to make it easy for people to prove their identity online, regardless of their location or the origin of their ID card.

Smile ID employs advanced facial recognition technology with a 99.8% accuracy rate across all skin tones. This ensures that the individual undergoing verification is physically present, effectively preventing spoofing attempts using photos, videos, or masks.

Socure

socure.com

Socure, established in 2012, is a private firm headquartered in Incline Village, Nevada, USA.

Socure's Predictive Document Verification product integrates passive liveness detection, which operates in the background without requiring users to perform specific actions like blinking or smiling, enhancing user experience while maintaining security. Its selfie feature to verify ID photos also includes liveness checks.

Spoofsense

spoofsense.ai

SpoofSense, founded in 2021, is headquartered in Jaipur, Rajasthan, India. The company specializes in AI-powered facial liveness detection, offering solutions to protect businesses from spoofing attacks.

SpoofSense achieved iBeta Level-2 compliance under the ISO 30107-3 standard, validating its effectiveness against sophisticated spoofing techniques such as 3D masks and high-quality video replays. By integrating these advanced features, SpoofSense enhances digital security, providing businesses with robust tools to prevent identity fraud across various industries, including banking, fintech, healthcare, and government services.

Sumsub

sumsub.com

Sumsub, established in 2015, is headquartered in London, United Kingdom and specializes in identity verification services.

Sumsub's liveness verification system utilizes a neural network to scan a user's face, creating a 3D map to analyze and adapt to various facial features.

Suprema

supremainc.com

Suprema, established in 2000, is headquartered in South Korea and specializes in biometric and security solutions, offering products such as access control systems and time and attendance devices.

The latest optical technology and Suprema's facial authentication algorithm accurately distinguish the faces of users.

Svort

svort.io

SVORT is a company specializing in neural-biometric access management systems. Its technology focuses on

creating an anonymous 3D model of a user's face, which is then linked to a personal neural network. This ensures that during authentication, both the user's identity and liveness are confirmed.

SVORT's solutions can be applied across various sectors including banking, software, healthcare, retail and government.

Sybrin

sybrin.com

Sybrin, founded in 1991, is headquartered in Fourways, South Africa. The company specializes in digital transformation solutions for the financial services, insurance, and telecommunications industries. Its offerings include identity verification, payments processing, customer communications management, document management, case management, and fraud risk management.

Sybrin provides both active and passive methods to verify that an individual is physically present during remote interactions and its liveness detection solutions are designed to conform to ISO/IEC 30107-3 standards and have been tested by FIME labs, receiving a letter of conformance in 2021.

T

Tech5

tech5.ai

Tech5, founded in 2018, is headquartered in Geneva, Switzerland and specializes in developing biometric and digital identity solutions, focusing on face, fingerprint, and iris recognition technologies.

Its offerings include contactless biometric capture, identification systems, and digital ID management platforms. Tech5 has developed the T5-LDS (Liveness Detection System), an AI-powered technology designed to perform real-time passive liveness checks for face and fingerprint images.

Thales

thalesgroup.com

Thales Group was established in 1893 and is headquartered in Paris, France.

Thales integrates liveness detection into its biometric and digital identity solutions to ensure security and prevent identity fraud.

Toppan

toppan.com

Toppan Inc., established in 2023, is headquartered in Tokyo, Japan. In 2020, Toppan expanded its capabilities in digital identity verification by acquiring the Taiwanese software company iDGate.

Toppan iDGate's face recognition SDKs and APIs enable comprehensive security and frictionless experiences. AI-based liveness detection allows for image processing and feature value comparisons with AI models.

Trinamix

trinamix.com

trinamiX GmbH, established in 2015, is a wholly owned subsidiary of BASF SE, headquartered in Ludwigshafen, Germany. trinamiX has developed a unique method of liveness detection that enhances biometric authentication security by detecting human skin.

This passive liveness detection technique is integrated into its face authentication solutions, ensuring that the system can distinguish between real human skin and artificial

representations, thereby preventing spoofing attempts.

Trustmatic

trustmatic.com

Trustmatic, founded in 2020, is headquartered in Bratislava, Slovakia. The company specializes in AI-powered identity verification and fraud detection solutions, assisting businesses in automating customer onboarding, ensuring compliance with KYC regulations, and preventing fraud. In November 2023, Trustmatic was acquired by Certn, a global leader in background screening and identity verification.

Trustmatic offers remote identity verification, face liveness detection and biometric identification to identify potential fraudsters by comparing images against databases of known offenders or previous onboarding sessions. Trustmatic's passive approach enhances user experience by eliminating the need for active participation, such as blinking or smiling. This method increases automation rates and reduces customer abandonment during the onboarding process.

U

Unico

unico.io

Unico, founded in 2007, is headquartered in São Paulo, Brazil and specializes in facial recognition and identification technology.

Unico has developed a liveness tool called SmartLive, which is integrated into its SDK and ensures that the individual is physically present during the selfie capture process.

Unissey

unissey.com

Unissey, founded in 2018, is headquartered in Paris, France and specializes in AI-driven facial biometric identity verification solutions.

Unissey's liveness detection solution has achieved compliance with the ISO 30107-3 standard for both mobile and desktop platforms.

V

Veridas

veridas.com

Veridas, founded in 2017, is headquartered in Tajonar, Spain.

It specializes in digital identity verification and biometric authentication solutions, offering proprietary technologies for facial and voice biometrics, identity document verification, and liveness detection.

Veriff

veriff.com

Veriff, founded in 2015, is a global identity verification company headquartered in Tallinn, Estonia.

The company specializes in providing AI-powered identity verification solutions and employs advanced passive liveness detection techniques to ensure that the individual undergoing verification is physically present during the authentication process.

VerifyMe

verifyme.ng

VerifyMe Nigeria, founded in 2013, is headquartered in Lagos, Nigeria. The

company specializes in digital identity verification and KYC technology solutions, aiming to bridge the credibility gap across Africa.

The company's biometric authentication solutions incorporate AI-powered facial recognition and liveness detection to ensure secure onboarding and e-commerce transactions.

VisionLabs

visionlabs.ai

VisionLabs, founded in 2012, is headquartered in Amsterdam, Netherlands. The company specializes in computer vision and machine learning, focusing on facial recognition technology.

VisionLabs' liveness detection technology is integrated into its products, such as the LUNA SDK and LUNA Platform, enabling efficient and accurate processing of images and live video streams for facial recognition.

Y

Yoti

yoti.com

Yoti, founded in 2014, is headquartered in London, United Kingdom and specializes in digital identity solutions, including identity verification, age estimation, and e-signatures.

Yoti's services are utilized across various sectors, such as finance, retail, and online services, to enhance security and streamline user authentication processes. Yoti has developed a proprietary technology called MyFace and this passive liveness detection solution ensures that the individual undergoing verification is physically present.

YouVerse

youverse.id

Youverse, founded in 2019, is headquartered in Lisbon, Portugal and specializes in developer-first facial biometric authentication solutions.

Youverse integrates liveness detection to ensure that the individual being authenticated is physically present during the verification process.

Z

Zoloz

zoloz.com

Zoloz, founded in 2012, is a global technology service provider specializing in AI-powered digital identity verification solutions.

The company was acquired by Ant Group in 2016. Zoloz's solutions include Real ID, Face Capture, and Connect, which integrate advanced biometric verification and liveness detection technologies.

BIOMETRIC UPDATE.COM

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS